DEFINE • DESIGN • **DEPLOY**

Zero Trust Network Access

SSL VPN to ZTNA Migration Guide

Version 7.2.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 14, 2023
Zero Trust Network Access 7.2.2 SSL VPN to ZTNA Migration Guide
01-722-765857-20230414

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-10-07	Initial release.
2023-04-14	Updated FortiAnalyzer on page 10.

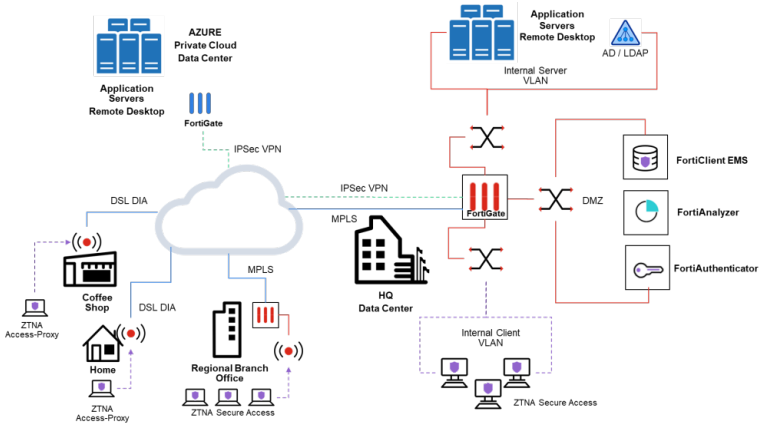
Deployment overview

This document provides a deployment example of Fortinet's Zero Trust Network Access (ZTNA) for hosted web applications, covering the following solutions:

- SSL VPN to ZTNA migration
  - Preparing your existing Fortinet SSL VPN solution to migrate to ZTNA
  - Overview of reusable components
- ZTNA Access Proxy for hosted Web applications
  - HTTPS access proxy solution and architecture
  - Applies to both remote access and internal access to Web applications hosted on the internal network
  - No persistent connection (such as VPN) is necessary

Using a similar scenario and topology example from the *ZTNA Architecture Guide*, we will walk through deploying the core components by providing configuration examples to help you migrate from SSL VPN to ZTNA access proxy for remote users accessing hosted web applications.

The goal is to reduce the reliance on dial-up and SSL VPN by adding device authentication with role-based application access. We will focus on the services located at head quarters (HQ) along with remote users currently using SSL VPN. Concepts from this deployment guide can be applied to regional offices and even cloud datacenters.



Audience

This migration guide is aimed at companies with existing SSL VPN teleworking solution deployed with the FortiGate and FortiClient looking to secure their remote access using ZTNA. Midlevel network and security architects in companies of all sizes and verticals should find this guide helpful. A working knowledge of FortiOS and the Fortinet Security Fabric is helpful.

About this guide

This deployment guide describes the steps involved in deploying a specific architecture. Readers should first evaluate their environment to determine whether the architecture outlined in this guide suits them. It is advisable to review the Reference Architecture Guide(s), such as the *ZTNA Architecture Guide*, if readers are still in the process of selecting the right architecture. See also the *ZTNA Concept Guide*.

This deployment guide presents one of possibly many ways to deploy the solution. It may also omit specific steps where readers must make design decisions to further configure their devices. It is recommended that readers also review supplementary material found in product administration guides, example guides, cookbooks, release notes, and other documents where appropriate on the Fortinet Document Library.

Design considerations

Traditionally, VPN is used to secure data flowing in an otherwise insecure connection. However, the method of access over VPN often doesn't account for the risk of infected or non-compliant endpoints infecting network devices. Given the greater risks of allowing remote devices into the network, their access is often limited.

ZTNA tackles some of these issues by securing your traffic over an SSL connection, validating the device identity, verifying that appropriate endpoint security features are turned on, and authenticating user identity. These measures help reduce security risk factors to give remote users a level of access similar to what is available when working locally in the office. This also gives rise to role-based application access, where access is granted based on the user and device roles, instead of the traffic source.

Migrating from SSL VPN to ZTNA

Organizations that have a mature SSL VPN solution in place likely have the following in common:

- Remote access users and groups are defined on an external server, for example, on a Windows Active Directory.
- Granular rules are defined to grant distinct user groups access to different resources.
- For scaling the VPN solution, SSL VPN is offered in tunnel mode to remote users.
- Remote users have FortiClient installed on their endpoints, and is actively managed by FortiClient EMS.

When the above criteria are met, the basic components and configurations for ZTNA is already in place. Namely, a FortiGate with various user groups defined and FortiClients provisioned and managed by EMS. Administrators can take a phased approach in migrating hosted servers and user groups to ZTNA while incrementally disabling access through SSL VPN.

See the *Product prerequisites* section for more information on the required and recommended components, and how they form the ZTNA solution.

ZTNA Access Proxy for hosted Web applications

With Web applications hosted on the internal network, ZTNA enables end users to access these applications directly and securely on the browser. Traffic to the destination servers are redirected to the FortiGate access proxy where device identity and posture checking occurs. The FortiGate then grants access and logs the connection.

ZTNA Access Proxy for hosted TCP Applications

ZTNA TCP forwarding access proxy is used for other applications, such as SSH, Remote Desktop Protocol (RDP), and others. The biggest difference in implementation is it requires the FortiClient endpoint to redirect the application request to the ZTNA access proxy using ZTNA mapping rules. These rules can be managed by FortiClient EMS and provisioned to FortiClient Endpoints automatically.

Summary

As discussed in the *ZTNA Architecture Guide*, when using ZTNA access proxy, it is important to consider when to apply HTTPS access proxy or TCP forwarding access proxy. Generally, web applications will fall under the former. Non-web applications, such as RDP, will fall under the latter, which is most useful for securing remote access. Remember the design goal for Zero Trust Network Access: a device inside the network is trusted no more than a device outside the network. With this in mind, we use ZTNA secure access features to check the posture of devices directly connected to internal network segments and verify the identity of the users accessing the applications locally.

For the purpose of this Deployment guide, we will cover the migration of hosted Web applications to ZTNA only.

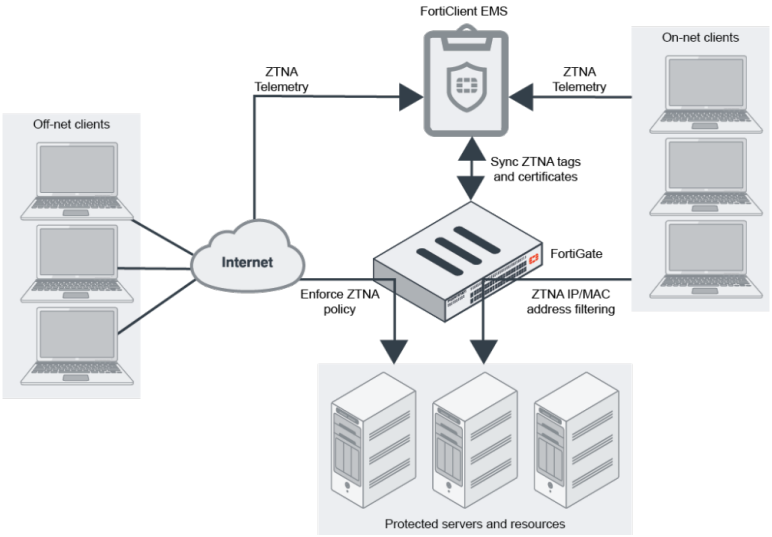
Success criteria

In the ZTNA design, the goal is to enhance security by improving identity and posture checking of devices connecting to the internal network, and by reducing the attack surface of traditional dial-up VPN. In our use case, the following success criteria is detailed:

- Block Unmanaged Devices and devices that cannot prove their identity (No device certificate).
- Allow only identified user groups access to only the specific applications that they need.
- For remote users, limit direct access to the internal network for web applications.
- Dynamically deny access to devices with critical vulnerabilities both on the internal network and remote.
- Dynamically allow access once the vulnerabilities are remediated.
- Reduce the reliance on dial-up and SSL VPN.
- Use a phased approach to migrate SSL VPN implementation to ZTNA.

Product prerequisites

The ZTNA solution is comprised of multiple products to establish device identity and device trust context. FortiClient, FortiClient EMS, and FortiGate are all integral to ZTNA, and used to establish device identity by using client certificates, device trust context, and user identity.



FortiClient

FortiClient is a required component for ZTNA. It gathers information about the endpoint and in some cases is used as an enforcement tool.

For licensing information, review the FortiClient data sheet found in FortiClient Endpoint Security Overview.

FortiClient endpoints provide the following information to FortiClient EMS when the endpoints register to FortiClient EMS:

- Device information (network details, operating system, model, and others)
- Logged on user information
- Security posture (On-net/Off-net, antivirus software, vulnerability status, and others)

FortiClient also requests and obtains a client device certificate from the EMS ZTNA Certificate Authority (CA) when it registers to FortiClient EMS. FortiClient uses the certificate to identify itself to the FortiGate.

FortiClient EMS

FortiClient EMS is a required component for ZTNA.

Licensing for FortiClient EMS is included with the FortiClient ZTNA license. See also FortiClient Endpoint Security Overview.

FortiClient EMS issues and signs the client certificate with the FortiClient UID, certificate serial number, and EMS serial number. The certificate is then synchronized to the FortiGate. FortiClient EMS also shares its EMS ZTNA CA certificate with the FortiGate, so that the FortiGate can use it to authenticate the clients.

FortiClient EMS uses Zero Trust tag rules to tag endpoints based on the information that it has on each endpoint. The tags are also shared with FortiGate.

FortiGate

FortiGate is a required component for ZTNA.

ZTNA Licensing is included with FortiOS. The minimum recommended license bundle is Unified Threat Protection, and the recommended license bundle is Enterprise Protection. See the data sheets found in Next-Generation Firewall.

FortiGate maintains a continuous connection to FortiClient EMS to synchronize endpoint device information, including:

- FortiClient UID
- FortiClient certificate serial number
- FortiClient EMS serial number
- Device credential (user/domain)
- Network (IP and MAC address and route to the FortiGate)

When a device's information changes, such as when a client moves from On-net to Off-net, or their security posture changes, FortiClient EMS is updated with the new device information, and then updates the FortiGate. FortiGate's wad daemon can use this information when processing ZTNA traffic.

FortiAnalyzer

FortiAnalyzer is a recommended component for ZTNA.

FortiAnalyzer is licensed by anticipated log volume. VM and hardware models are available. For details, see the data sheet found in FortiAnalyzer Overview.

FortiAnalyzer is used for gathering and analyzing logs as well as generating reports for Fortinet devices. FortiAnalyzer should be available from everywhere. FortiAnalyzer receives logs directly from FortiClient, and FortiAnalyzer is integral for analyzing and reporting on users and devices connected to the network. Optional SOC services are invaluable for quickly reacting to IOCs and other related security events.

FortiAuthenticator and FortiToken (recommended)

FortiAuthenticator and FortiToken are recommended components for ZTNA, but they are not required.

For licensing information, review the FortiAuthenticator and FortiToken data sheets.

FortiAuthenticator provides network and user identity authentication services to all ZTNA components. It also incorporates multi-factor authentication through FortiToken and FortiToken Cloud. By centralizing authentication services within FortiAuthenticator, the ZTNA solution can easily scale as different components connect without duplicating user configurations.

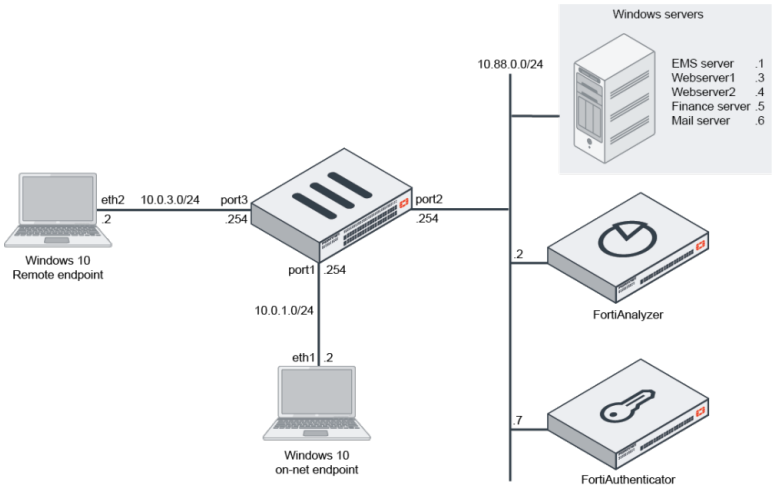
Additional component information

ZTNA Solution	Licensing	Existing Infrastructure
FortiClient ZTNA client 7.0 and above	Review the FortiClient data sheet	Available deployment techniques include: an existing software deployment tool (for example, SCCM), native deployment through FortiClient EMS (Windows only), and a manual download location accessible for outliers.

ZTNA Solution	Licensing	Existing Infrastructure
FortiClient Endpoint Management Server (EMS) 7.0 and above	Included with FortiClient ZTNA license	FortiClient EMS must be accessible to clients from everywhere. In this design, FortiClient EMS is deployed in a DMZ. Active Directory integration to FortiClient EMS may also be necessary for client deployment and ease of applying different endpoint profiles to corresponding groups in AD.
FortiOS ZTNA Access Proxy 7.0 and above	Included with FortiOS Minimum recommended bundle is Unified Threat Protection Recommended bundle is Enterprise Protection	Review FortiGate performance requirements, and ensure existing FortiGates meet those requirements. In this simple deployment example, the FortiGate and Security Fabric are central to all traffic and to protect traffic flow to critical resources.
FortiOS Identity Service Provider (SP)	Included with FortiOS	The FortiGate acts as an SP and integrates with FortiAuthenticator as an IdP broker, providing integration to Active Directory and MFA services with SAML.
FortiAuthenticator Identity and Access Management (IAM)	Review FortiAuthenticator data sheet	When multiple FortiGates are deployed, FortiAuthenticator is desirable to consolidate and manage connections to IdPs, including Active Directory, LDAP, Radius, and SAML providers. In this use case, FortiAuthenticator is not strictly necessary, but is included in the deployment as an example for larger deployments.
FortiToken Multi-factor Authentication (MFA)	Review FortiToken data sheet	MFA is recommended for connecting to any critical resources. In addition to device and user authentication, another factor of authentication that utilizes one-time passwords (OTP) is desirable to help protect against stolen credentials. An existing OTP product can be integrated through SAML. In this deployment, we apply FortiToken to users in FortiAuthenticator. In smaller, single FortiGate organizations, FortiToken can be managed directly on the FortiGate.
FortiAnalyzer	Review FortiAnalyzer data sheet. VM and hardware models available. License by anticipated log volume.	FortiAnalyzer is recommended for gathering logs, analyzing logs, and generating reports for Fortinet devices. FortiAnalyzer should be available from everywhere. FortiClient ZTNA sends logs directly to FortiAnalyzer.

Deployment procedures

The deployment example has the following topology:



In this example topology, a customer has several servers running in their internal corporate network. Web access to the servers are divided by user groups.

User	AD User Group	Access
FortiAD\Tom Smith (tsmith)	Sales	Webserver1 Webserver2
FortiAD\Dan Parker (dparker)	Finance	Webserver1 Webserver2 Finance server
FortiAD\Administrator	Administrators	Webserver1 Webserver2 EMS server FortiAnalyzer FortiAuthenticator

User authentication is managed by Windows Active Directory. Each user logs into the FortiAD domain for authentication on their workstation. FortiGate integrates with Windows AD via a LDAPS connection and uses the same user groups for SSL VPN and ZTNA.

The web mail server is accessible by all via a Virtual IP. The EMS server registration and telemetry service (TCP/8013) is also accessible by all via a Virtual IP. They do not require SSL VPN or ZTNA policies to access.

The FortiAuthenticator is optional in this environment. It can be used to provide different types of authentication such as SAML or RADIUS, or provide MFA via FortiTokens or email OTP. In this Deployment Guide, the FortiAuthenticator is not used for authentication. However it is used to demonstrate a Web application accessible by the Administrators group.

Lastly, this topology simulates on-net users in the 10.0.1.0/24 network, using a default DNS server on 10.88.0.1. Off-net remote users on the other hand are on the 10.0.3.0/24 network, using the FortiGate 10.0.3.254 as its default DNS server. Users should have the same level of access whether on-net or off-net.

Migrating from SSL VPN to ZTNA for hosted Web Applications

Before migration can occur, we must examine the current SSL VPN configuration and topology, assess components and configurations that can be re-used, and then prepare the components for ZTNA. Migrations is performed one server at a time, starting with servers accessible by the least number of users and groups.

This chapter will walk through the following:

1. Existing teleworking configurations on page 13
2. Prepare FortiClient and FortiClient EMS for ZTNA on page 17
3. Migrate Web access to infrastructure devices for Administrators on page 22
4. Migrate Web access to Finance server for Finance group on page 32
5. Migrate Web access to Webserver1 and Webserver2 on page 39
6. Configuring and verifying rules for on-net access on page 46
7. Shut off all SSL VPN access on page 53

The goal is to apply device identity and posture check to prevent unauthorized devices or vulnerable devices from accessing the hosted Web applications. Security posture check in our example amounts to the following:

- Devices are checked for critical vulnerabilities. If critical vulnerabilities exist, devices cannot be trusted.
- Devices are checked for domain registration. They must be registered to the company's Active Directory domain.

Existing teleworking configurations

The following assumptions are made regarding the existing Teleworking solution:

- Remote access users and groups are defined on an external server, likely on a Windows Active Directory.
- Granular rules are defined to grant distinct user groups access to different resources.
- For scaling the VPN solution, SSL VPN is offered in tunnel mode to remote users.
- Remote users have FortiClient installed on their endpoints, and is actively managed by FortiClient EMS.

Let's examine the existing configurations.

Remote access users and groups

In our example company, users are stored in Windows Active Directory under the FortiAD.Info domain. PCs must be logged into this domain, and remote users also use the same credentials to connect to SSL VPN.

The FortiGate connects to the Windows Active Directory via a LDAPS connection. The configurations for our LDAP server settings on the FortiGate is as follows:

```
config user ldap
    edit "LDAP-fortiad"
        set server "10.88.0.1"
        set cnid "sAMAccountName"
        set dn "dc=fortiad,dc=info"
        set type regular
        set username "fortiad\\Administrator"
        set password <password>
        set secure ldaps
        set ca-cert "CA_Cert_1"
        set port 636
    next
end
```

The following are the User Group configurations on the FortiGate:

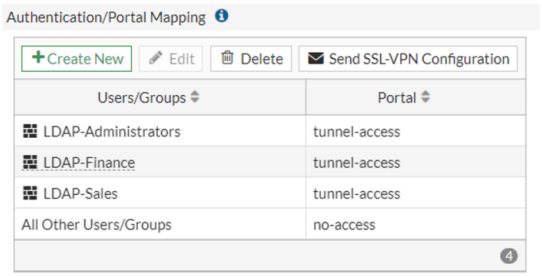
Group Name	Group Type	Members
LDAP-Administrators	Firewall	LDAP-fortiad
LDAP-Finance	Firewall	LDAP-fortiad
LDAP-Sales	Firewall	LDAP-fortiad

```
config user group
    edit "LDAP-Administrators"
        set member "LDAP-fortiad"
        config match
            edit 1
                set server-name "LDAP-fortiad"
                set group-name "CN=Administrators,CN=Builtin,DC=fortiad,DC=info"
            next
        end
    next
    edit "LDAP-Finance"
        set member "LDAP-fortiad"
        config match
            edit 1
                set server-name "LDAP-fortiad"
                set group-name "CN=Finance,CN=Users,DC=fortiad,DC=info"
            next
        end
    next
    edit "LDAP-Sales"
        set member "LDAP-fortiad"
        config match
            edit 1
                set server-name "LDAP-fortiad"
                set group-name "CN=Sales,CN=Users,DC=fortiad,DC=info"
            next
        end
    next
end
```

SSL VPN tunnel mode configurations

SSL VPN is configured to offer tunnel mode access via the WAN (port3) interface. All three user groups are configured to map to the tunnel-access portal.

The SSL VPN *Authentication/Portal Mapping* are as follows:




```
config vpn ssl settings
    set servercert "ztna-wildcard"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set dns-server1 10.88.0.1
    set source-interface "port3"
    set source-address "all"
    set source-address6 "all"
    set default-portal "no-access"
    config authentication-rule
        edit 1
            set groups "LDAP-Administrators"
            set portal "tunnel-access"
        next
        edit 2
            set groups "LDAP-Finance"
            set portal "tunnel-access"
        next
        edit 3
            set groups "LDAP-Sales"
            set portal "tunnel-access"
        next
    end
end
```

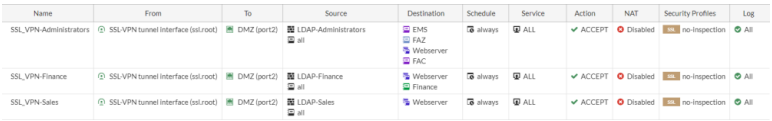
Addresses and address groups

Addresses and address groups are created for each server or group of servers.

Name	Details	Type
IP Range/Subnet 7/14		
EMS	10.88.0.1/32	Address
FAC	10.88.0.7/32	Address
FAZ	10.88.0.2/32	Address
Finance	10.88.0.5/32	Address
MailServer	10.88.0.6/32	Address
Webserver1	10.88.0.3/32	Address
Webserver2	10.88.0.4/32	Address
FQDN 1/7		
webserver.ztnademo.com	webserver.ztnademo.com	Address
Address Group 1/3		
Webserver	Webserver1 Webserver2	Address Group

Granular firewall rules

Firewall rules are configured to provide granular remote access for each group of users. They are configured as follows:

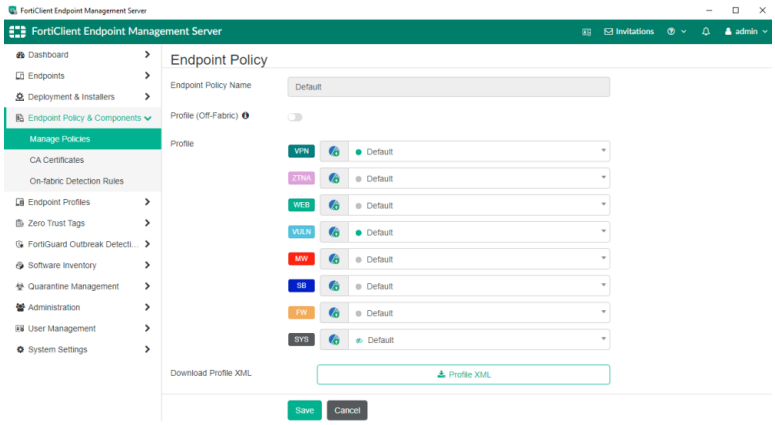


Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
SSL_VPN-Administrators	SSL-VPN tunnel interface (ssl.root)	DMZ (port2)	LDAP-Administrators all	EMS FAZ Webserver FAC	always	ALL	ACCEPT	Disabled	no-inspection	All
SSL_VPN-Finance	SSL-VPN tunnel interface (ssl.root)	DMZ (port2)	LDAP-Finance all	Webserver Finance	always	ALL	ACCEPT	Disabled	no-inspection	All
SSL_VPN-Sales	SSL-VPN tunnel interface (ssl.root)	DMZ (port2)	LDAP-Sales all	Webserver	always	ALL	ACCEPT	Disabled	no-inspection	All

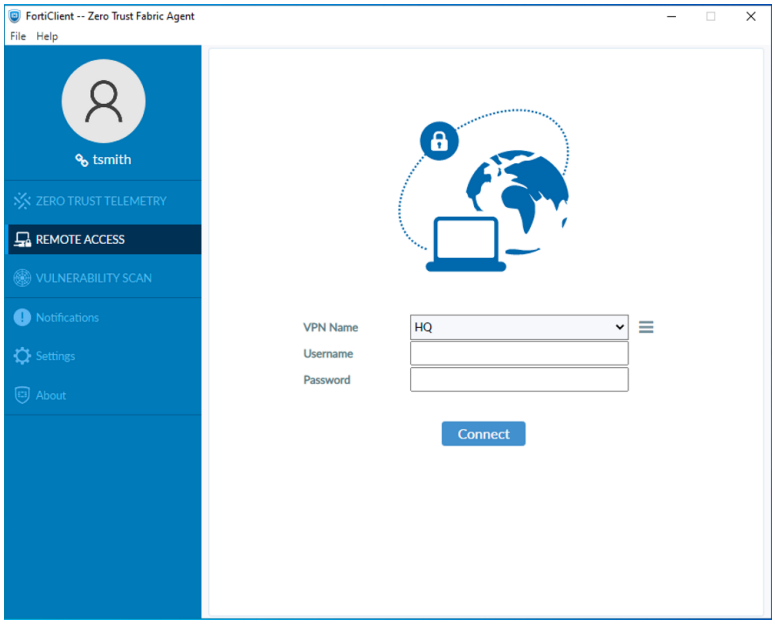
```
config firewall policy
    edit 9
        set name "SSL_VPN-Administrators"
        set srcintf "ssl.root"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "EMS" "FAZ" "Webserver" "FAC"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set groups "LDAP-Administrators"
        set comments " "
    next
    edit 10
        set name "SSL_VPN-Finance"
        set srcintf "ssl.root"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "Webserver" "Finance"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set groups "LDAP-Finance"
        set comments " "
    next
    edit 11
        set name "SSL_VPN-Sales"
        set srcintf "ssl.root"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "Webserver"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set groups "LDAP-Sales"
        set comments " "
    next
end
```

FortiClient Endpoint management with FortiClient EMS

FortiClients are managed by FortiClient EMS under the same endpoint policy configurations (Default). The policy has VPN, Vulnerability Scan, and the System Settings profile enabled.



The FortiClient Endpoint allows SSL VPN remote access.



Prepare FortiClient and FortiClient EMS for ZTNA

Configurations in the previous section for SSL VPN offer a good basis for the ZTNA configuration and migration. However, a bit more configuration is required.

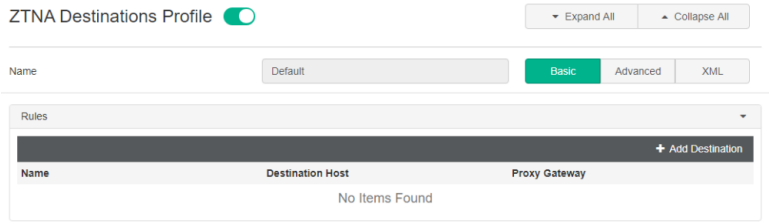
1. Push ZTNA endpoint profile from EMS to FortiClient Endpoints on page 18
2. Configure Zero Trust Tags to the FortiGate on page 19
3. Configure a Fabric connector on the FortiGate to connect to FortiClient EMS on page 21
4. Synchronize Zero Trust Tags to the FortiGate on page 22

Push ZTNA endpoint profile from EMS to FortiClient Endpoints

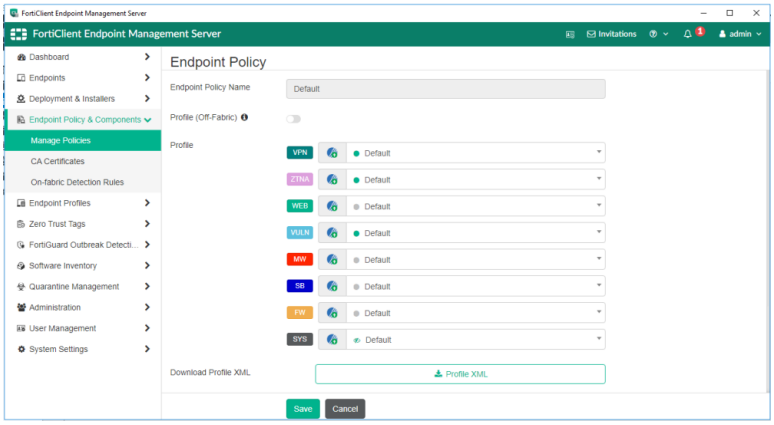
Because ZTNA requires EMS to act as the ZTNA Certificate Authority and issue client certificates to each device, the FortiClient Endpoints must have the ZTNA module installed. This is not necessary for strictly SSL VPN remote access.

To push the ZTNA endpoint profile from FortiClient EMS:

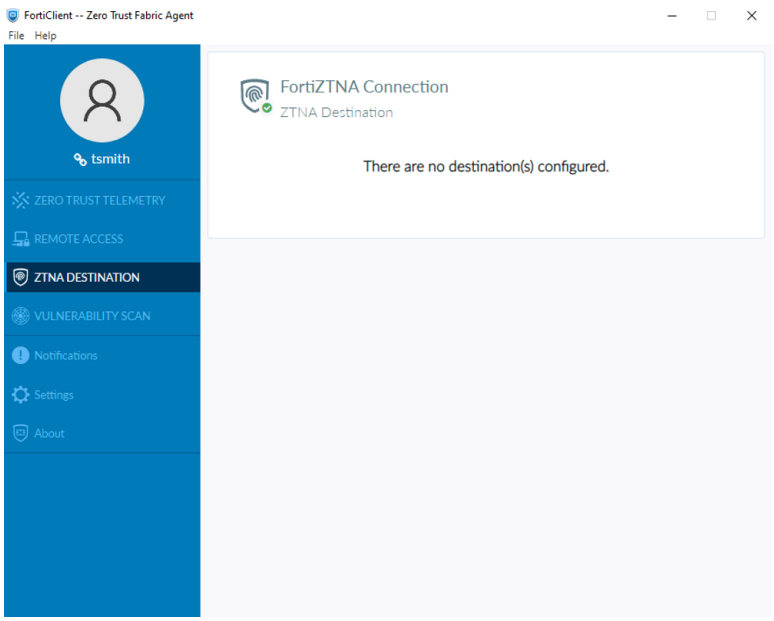
1. Under *Endpoint Profiles* > *ZTNA Destinations*, edit the *Default* profile.
2. At the very top, toggle the *ZTNA Destinations Profile* from *Disable* to *Enable*.



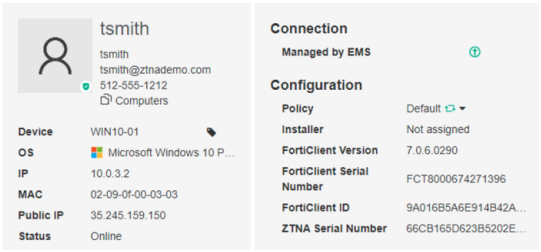
3. For ZTNA hosted Web Access, this is the only configuration needed. Click *Save* to save the changes.
4. Under *Endpoint Policy & Components* > *Manage Policies*, edit the *Default* policy.
5. Ensure that the *Default* profile is assigned to *ZTNA*.
6. Click *Save* to complete.



From a registered FortiClient endpoint, verify that the client has received the updates. The *ZTNA Destination* should now be installed.



Back on the FortiClient EMS, view the managed endpoint from Endpoints > All Endpoints. The user device should appear as connected and *Managed by EMS*, and the ZTNA status has changed from disable to a valid *ZTNA Serial Number*.



Configure Zero Trust Tags to the FortiGate

Zero Trust tagging rules are used to perform endpoint posture check on the FortiClients. This info is synchronized to the FortiGate so that it can make the policy decision on whether to allow the device access to the protected resources.

This example uses two tagging rules for security posture check.

To configure a Zero Trust Tagging Rule to detect the presence of critical vulnerabilities:

1. Go to *Zero Trust Tags* > *Zero Trust Tagging Rules*.
2. On the top right, click *+Add*.
3. Enter name "`Critical Vulnerabilities`".
4. For *Tag Endpoint As*, type in `Critical_Vulnerabilites` and then hit `Enter` to create the Tag.
5. Click *Add Rule*.
   a. Select *Windows OS*.
   b. Select *Rule Type "Vulnerable Devices"*.

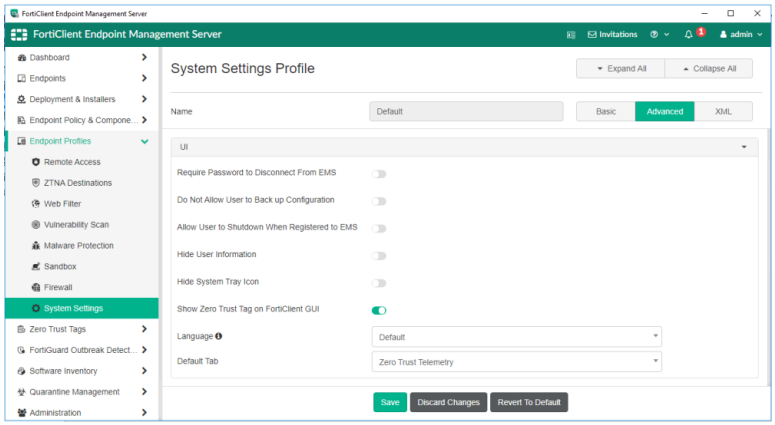
   c. Set *Severity Level to "Critical"*.
   d. Click *Save*.
6. Click *Save* to save this Zero Trust Tagging Rule.

To configure a Zero Trust Tagging Rule for detecting logged in Active Directory Domain - FortiAD.info:

1. Remain in *Zero Trust Tagging Rules* page.
2. On the top right, click *+Add*.
3. Enter name "`FortiAD.Info`".
4. For *Tag Endpoint As*, type in `FortiAD.Info` then hit *Enter* to create the Tag.
5. Click *Add Rule*.
   a. Select *Windows OS*.
   b. Select *Rule Type "Logged In Domain"*.
   c. Set *Domain FortiAD.Info*.
   d. Click *Save*.
6. Click *Save* to save this Zero Trust Tagging Rule.

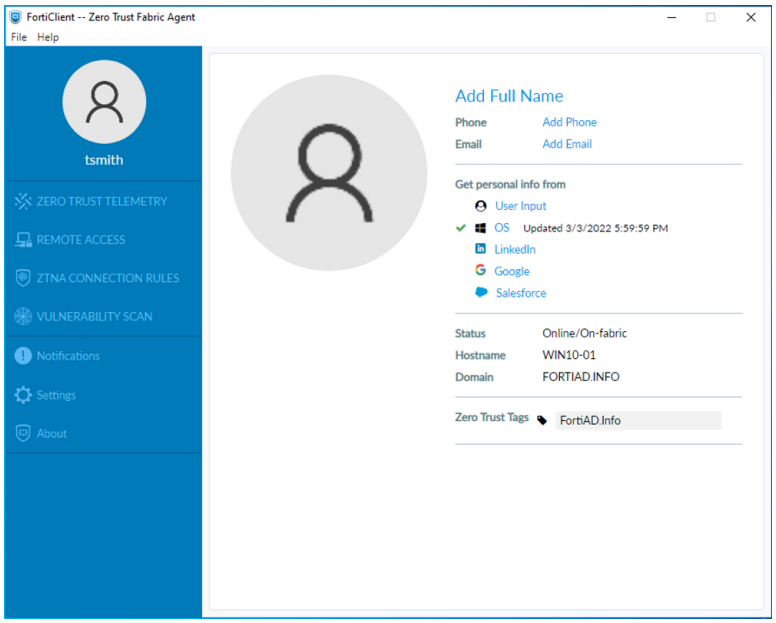
To configure the ZTNA tag to display on the FortiClient:

1. Remain in EMS and navigate to *Endpoint Profiles* > *System Settings*.
2. Edit the *Default* profile.
3. Be sure *Advanced settings* is selected (top right of window).
4. Under *UI*, enable *Show Zero Trust Tag on FortiClient GUI*.
5. Click *Save*.

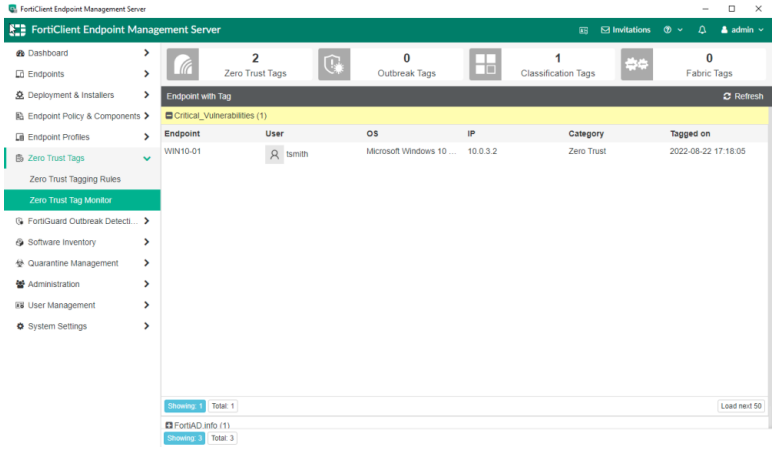


Verification:

1. On the FortiClient, click on the User avatar. This will show currently detected *Zero Trust Tags*.



2. Back on FortiClient EMS, navigate to *Zero Trust Tags* > *Zero Trust Tag Monitor*.
3. Refresh to display *Endpoints* that have been tagged by the Tagging rule.



Configure a Fabric connector on the FortiGate to connect to FortiClient EMS

In this example, the FortiClient EMS is on premise, so the FortiGate can be configured as follows.

To add an on-premise FortiClient EMS server in the GUI:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Click *Create New* and click *FortiClient EMS*.
3. Enter a name for the connector and the IP address or FQDN of the EMS.
4. Click *OK*.

5. A window appears to verify the EMS server certificate. Click *Accept*.
   See FortiClient EMS for more information.

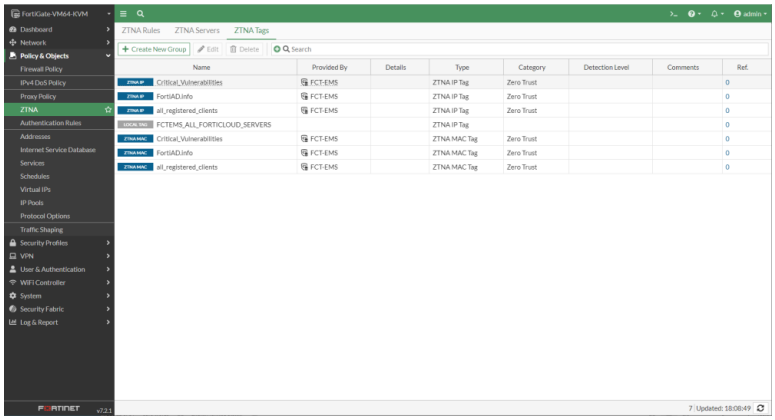
To add an on-premise FortiClient EMS server in the CLI:

```
config endpoint-control fctems
    edit <name>
        set server <server IP or domain>
    next
end
```

To configure the FortiGate to connect to FortiClient EMS Cloud, see the following topic.

Synchronize Zero Trust Tags to the FortiGate

1. On the FortiGate, go to *System* > *Feature Visibility* and enable *Zero Trust Network Access*.
2. Go to *Policy & Objects* > *ZTNA*. Then navigate to the *ZTNA Tags* tab.
   ZTNA tags that were created in EMS should be displayed on the page.



Migrate Web access to infrastructure devices for Administrators

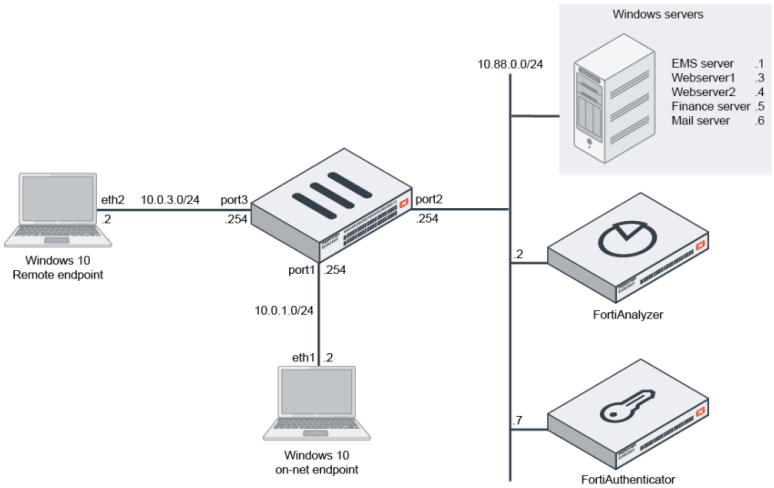
Migration is typically arranged so that the least number of users are impacted at first, before incrementally increase in scope. Therefore, it often begins with the servers and devices accessible only to the Administrator group themselves.

In our example, web access to the EMS server, FortiAnalyzer and FortiAuthenticator for the Administrators group will be migrated first. These servers are only accessible by Administrators. In the Teleworking setup, this corresponds to the following policy configurations:

```
config firewall policy
    edit 9
        set name "SSL_VPN-Administrators"
        set srcintf "ssl.root"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "EMS" "FAZ" "Webserver" "FAC"
```

```
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set groups "LDAP-Administrators"
        set comments " "
    next
next
```

In the above Teleworking configs, the Webserver address group is also allowed. However, this will be migrated last.



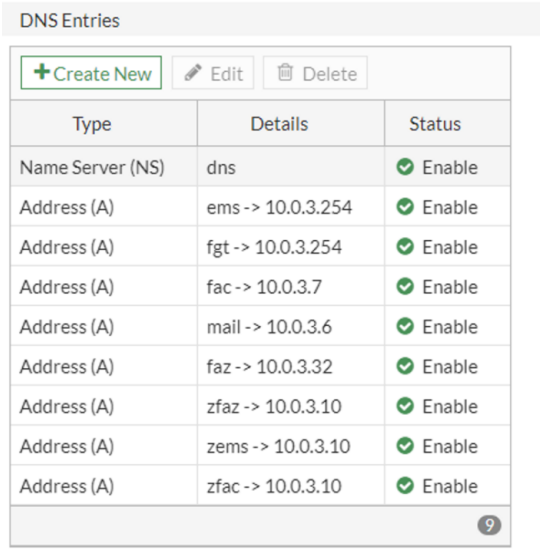
When we migrate to ZTNA, we will require the following:

- One new IP for port3 to act as the access proxy gateway. In our example environment, it is 10.0.3.10. In a production environment, this will likely be a public IP.
- For each web service, a FQDN and DNS entry to map the FQDN to the new IP above:
  - FortiAnalyzer – zfaz.ztnademo.com
  - FortiClient EMS – zems.ztnademo.com
  - FortiAuthenticator – zfac.ztnademo.com
- For HTTPS access to these services, a wildcard certificate for *.ztnademo.com

DNS configurations

It may be the case where each of the devices already have a FQDN defined on an internal DNS with the same name to facilitate access using SSL VPN. In this case, the internal definitions can remain the same. However, when resolved from remote, the FQDN needs to map to the IP address of the FortiGate access proxy. Therefore, it is advisable for the FQDN to be defined on an external DNS.

In our example, the FortiGate acts as a DNS server for remote clients with A records for mapping the above FQDNs to the access proxy address of 10.0.3.10. We will add the entries in our *Network* > *DNS Servers* > *DNS Database* settings.



ZTNA server configurations

One of the first essential steps is defining the ZTNA server. In our ZTNA server definition, we will apply the external IP of 10.0.3.10 on port 443. Then we will create 3 HTTPS server mappings to our respective services.

To configure the ZTNA server from GUI:

1. Under *Policy & Objects* > *ZTNA*, go to the *ZTNA Servers* tab.
2. Click *Create New* to create a new entry.
3. Input the following:

Name	ZTNA Webserver
External Interface	port3
External IP	10.0.3.10
External port	443
External certificate	1. Choose the wildcard certificate that applies to your domain. In our example, *ztna-wildcard*.

4. Under *Services/servers mapping*, click *Create new*.
5. For FortiAnalyzer web access enter the following and click *OK*:

Service	HTTPS
Virtual Host	Specify
Match By	Substring
Host	1. zfaz.ztnademo.com
Use certificate	1. ztna-wildcard

Server	Click *Create New*, input the following, and click *OK*: • Type: *IP* • IP: *10.88.0.2* • Port: *443* • Status: *Active*

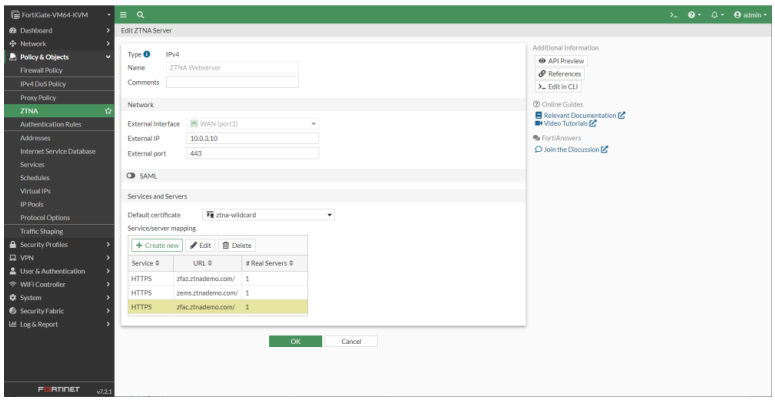
6. For FortiClient EMS web access enter the following and click *OK*:

Service	HTTPS
Virtual Host	Specify
Match By	Substring
Host	zems.ztnademo.com
Use certificate	1. ztna-wildcard
Server	Click *Create New*, input the following, and click *OK*: • Type: *IP* • IP: *10.88.0.1* • Port: *443* • Status: *Active*

7. For FortiAuthenticator web access, enter the following and click *OK*:

Service	HTTPS
Virtual Host	Specify
Match By	Substring
Host	zfac.ztnademo.com
Use certificate	1. ztna-wildcard
Server	Click *Create New*, input the following, and click *OK*: • Type: *IP* • IP: *10.88.0.7* • Port: *443* • Status: *Active*

8. Click *OK* to finish.



Authentication scheme and rules

User authentication helps define users and groups for role based access control. An authentication scheme and rule must be configured to trigger user authentication. The authentication scheme defines what method of authentication will be applied. An authentication rule specifies which proxy sources and destinations will require authentication, and which authentication scheme to apply.

This step demonstrates basic authentication using an LDAP server that connects to the Active Directory on our Windows server 10.88.0.1. In our topology, the LDAP server *LDAP-fortiad* used for SSL VPN access can be reused for ZTNA.

To configure an authentication scheme from GUI:

1. Go to *Policy & Objects* > *Authentication Rules* and select *Authentication Schemes* from the top right.
2. Click *Create New* > *Authentication Scheme*.
3. Enter the name `ZTNA Auth Scheme`.
4. Select *Method Basic*.
5. Change *User Database* to *Other*.
6. Select the LDAP server *LDAP-fortiad*.
7. Click *OK* to complete.

To configure an authentication rule from GUI:

1. Click *Create New* > *Authentication Rules*.
2. Enter the name `ZTNA Auth Rule`.
3. Select *Source Address* to *all*.
4. Set *Incoming interface* to *WAN (port3)*.
5. Leave *Protocol* as *HTTP*.
6. Click to *Enable Authentication Scheme* and select *ZTNA Auth Scheme*.
7. *IP-based Authentication* should be set to *Enable*.
8. *Enable This Rule* should be set to *Enable*.
9. Click *OK* to complete.

ZTNA rule configuration

Once the servers, authentication scheme and rules are configured, we will create ZTNA rules to control access. To recap, ZTNA rules help control access by defining users and ZTNA tags to perform user authentication and security posture checks. And just like firewall policies, you can granularly control the source and destination addresses, and apply appropriate security profiles to scan the traffic.

In this step, we will create a rule to deny endpoints whose security is compromised, identified by the presence of the *Critical_Vulnerabilities* tag. We will create a rule to allow users who are logged into the FortiAD.Info domain, identified by the presence of the *FortiAD.Info* tag. We will apply the policies for the existing *LDAP-Administrators* group, which is used in the SSL VPN policy.

To configure a ZTNA Rule for denying access:

1. In FortiOS, go to *Policy & Objects* > *ZTNA*, click the *ZTNA Rules* tab.
2. Click *Create New* to create a new rule.
3. In the *Name* box, type `ZTNA Deny Access`.
4. In the *Incoming Interface* list, select *WAN (port3)*.
5. In the *Source* list, select the following options:
   - For *Address*, select *all*.
   - For *User*, select *LDAP-Administrators*.

   When you define a user group, users would need to be authenticated first before their ZTNA tag is checked. The advantage is the username will be recorded in the violation log.
6. In the *ZTNA Tag* list, select the *Critical_Vulnerabilities* tag.
7. In the *ZTNA Server* list, select *ZTNA Webserver*.
8. In the *Destination* list, select the address objects *EMS*, *FAC* and *FAZ*.
9. Beside *Action*, select *Deny*.
10. Enable *Log Violation Traffic*.
11. Enable *Enable* this policy.
12. Click *OK* to complete.

To configure a ZTNA Rule for allowing access:

1. On the *Policy & Objects* > *ZTNA* > *ZTNA Rules* pane, click *Create New*.
2. In the *Name* box, enter `ZTNA-Administrators`.
3. In the *Incoming Interface* list, select *WAN (port3)*.
4. In the *Source* list, select the following options:
   - For *Address*, select *all*.
   - For *User*, select *LDAP-Administrators*.
5. In the *ZTNA Tag* list, select the *FortiAD.Info* tag.
6. In the *ZTNA Server* list, select *ZTNA Webserver*.
7. In the *Destination* list, select the address objects *EMS*, *FAC* and *FAZ*.
8. Beside *Action*, select *Accept*.

9. Enable *Security Profiles* as desired.
10. In the *Logging Options* section, enable *Log Allowed Traffic*, and select *All Sessions*.
11. Enable *Enable this policy*.
12. Click *OK* to complete.

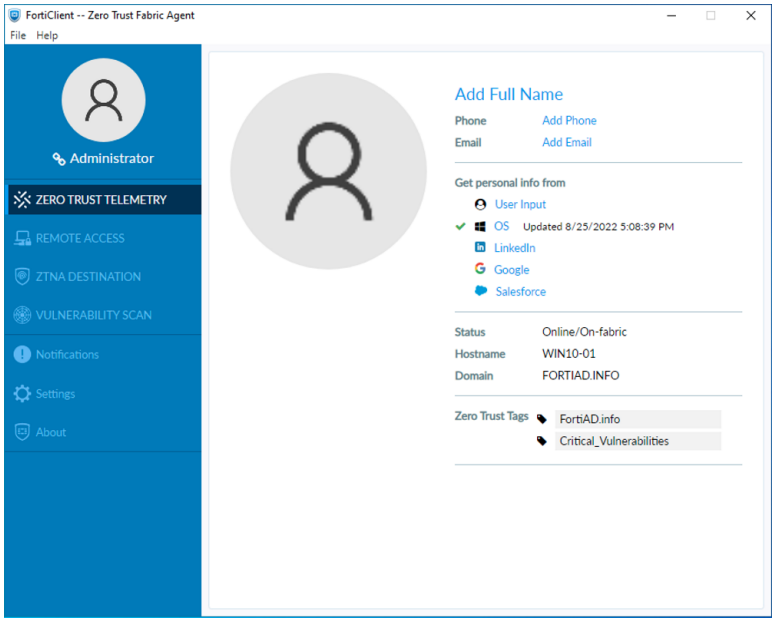
Testing and verification

Once the above configurations are completed, it is time to test ZTNA remote access on a workstation. Two test cases will be performed.

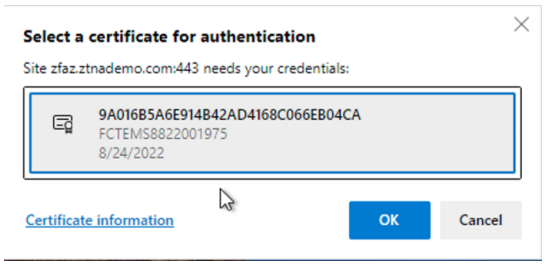
1. Verify access is denied when Critical Vulnerabilities are present on the PC
2. Verify access is allowed when Critical Vulnerabilities are resolved, and user is logged into the FortiAD domain.

To verify access is denied:

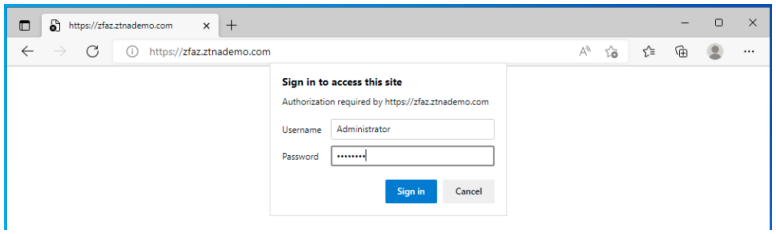
1. On an administrator's workstation, login to the FortiAD domain.
2. Open the *FortiClient > Zero Trust Telemetry* page.
3. Enter the *EMS address* or the invitation code. Connect to EMS.
4. Once EMS is connected, click the avatar to identify the current *Zero Trust Tags* assigned to this PC.



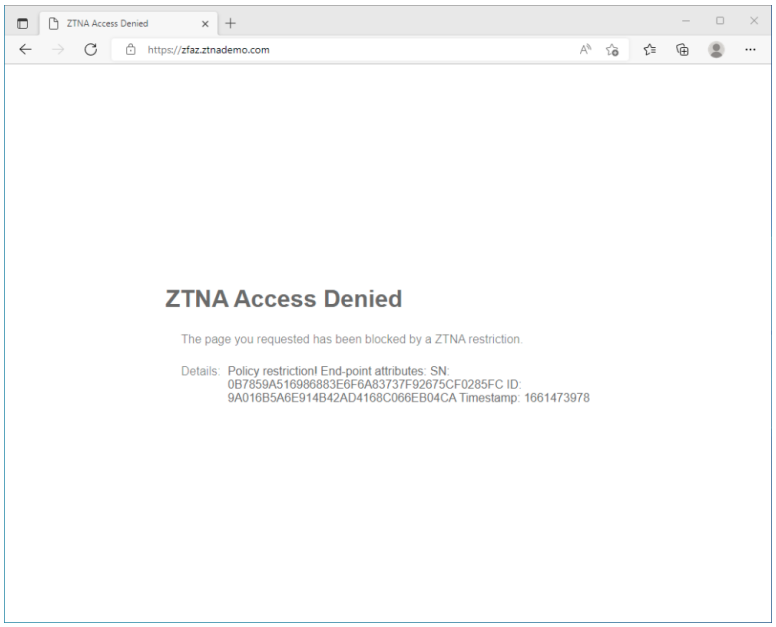
5. Open a browser, and enter the URL https://zfaz.ztnademo.com.
6. The browser will first prompt for the client certificate you want to use for this connection. Select the client certificate and press *OK*.



7. Next, the browser will prompt you for your user credentials. Enter your LDAP/Active Directory to continue.



8. If user authentication passes, the ZTNA rule will then assess the ZTNA tags. Since this workstation has Critical Vulnerabilities, access to the FortiAnalyzer is denied.



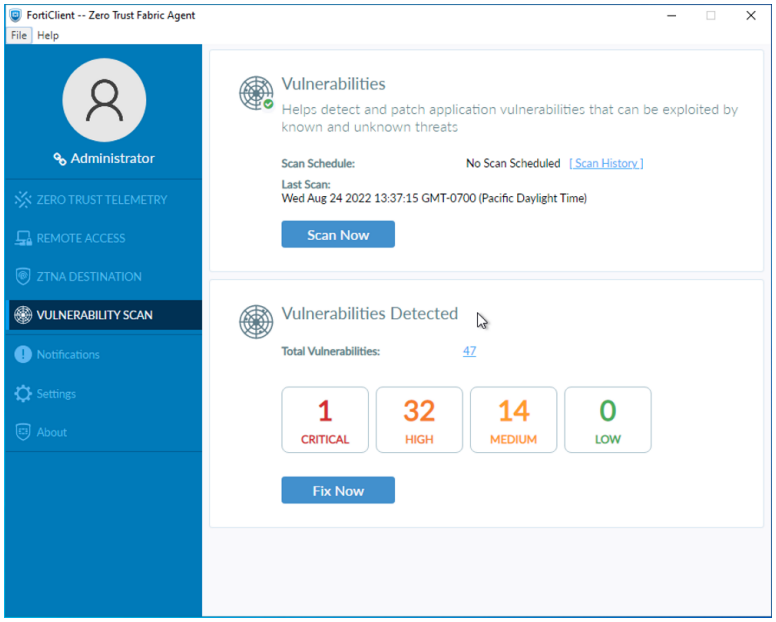
9. On the FortiGate, view the corresponding logs under *Log & Report* > *ZTNA Traffic*, or from the CLI:

```
# execute log filter category traffic

# execute log filter field subtype ztna

# execute log display

68 logs found.

10 logs returned.

2.0% of logs has been searched.

1: date=2022-08-25 time=17:36:29 eventtime=1661474189533247783 tz="-0700"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2
srcport=58729 srcintf="port3" srcintfrole="wan" dstcountry="Reserved"
```

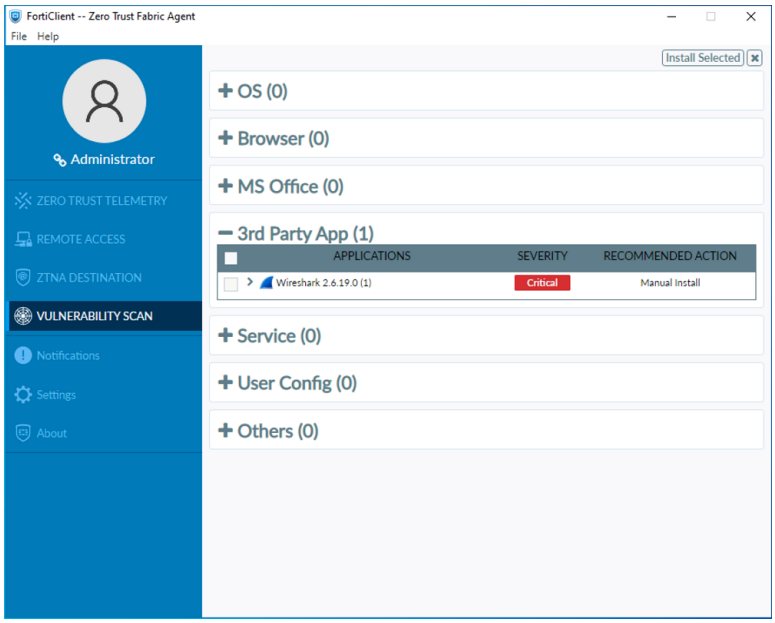
```
srccountry="Reserved" dstip=10.0.3.10 dstport=443 dstintf="root" dstintfrole="undefined"
sessionid=232642 srcuuid="32b4d66c-9426-51ec-be9c-9b0879d5b527" dstuuid="8cbf3c68-f75d-
51ea-4533-3cd1379a79dc" service="HTTPS" proto=6 action="deny" policyid=2
policytype="proxy-policy" poluuid="9b5aa784-9514-51ec-22d8-290ec0314a08"
policyname="ZTNA Deny Access" duration=211 user="Administrator" group="LDAP-
Administrators" authserver="LDAP-fortiad" vip="ZTNA Webserver" accessproxy="ZTNA
Webserver" clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA" clientdevicetags="on-
line/MAC_EMS1_ZTNA_Critical_Vulnerabilities/EMS1_ZTNA_FortiAD.info/MAC_EMS1_ZTNA_all_
registered_clients" msg="Denied: proxy-policy action is deny. Matched tag: EMS1_ZTNA_
Critical_Vulnerabilities" wanin=0 rcvdbyte=0 wanout=0 lanin=2839 sentbyte=2839
lanout=10114 fctuid="9A016B5A6E914B42AD4168C066EB04CA" appcat="unscanned" crscore=30
craction=131072 crlevel="high"
```

To verify access is allowed:

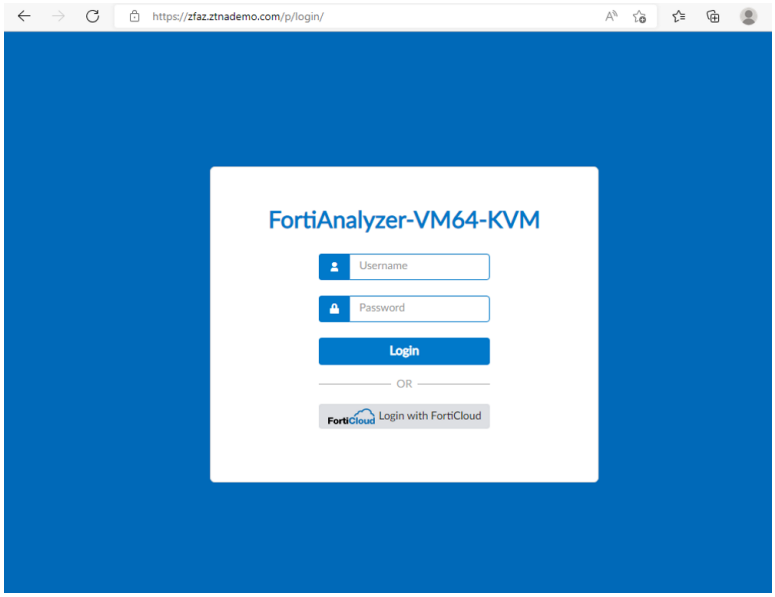
1. Open the *FortiClient* > *Vulnerability Scan* page.



2. Click on *Critical* to see the Application that has been identified with a critical vulnerability.



3. Apply the necessary fix to remove the vulnerability. Then perform a vulnerability scan.
4. Now that the workstation does not have a critical vulnerability, open your browser again to try accessing the FortiAnalyzer again.
5. Open a browser, and enter the URL https://zfaz.ztnademo.com.
6. If prior device certificate and user authentication are still valid, you will have access to your FortiAnalyzer right away. In not, select your device certificate and enter your user credentials. You should be able to access your FortiAnalyzer.



7. From the FortiGate, view the corresponding logs under *Log & Report* > *ZTNA Traffic*, or from the CLI:

```
# execute log filter category traffic
# execute log filter field subtype ztna
# execute log display
```

```
73 logs found.

10 logs returned.

2.0% of logs has been searched.

1: date=2022-08-25 time=17:55:17 eventtime=1661475317602317498 tz="-0700"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2
srcport=58807 srcintf="port3" srcintfrole="wan" dstcountry="Reserved"
srccountry="Reserved" dstip=10.88.0.2 dstport=443 dstintf="port2" dstintfrole="dmz"
sessionid=234555 srcuuid="32b4d66c-9426-51ec-be9c-9b0879d5b527" dstuuid="8cbf3c68-f75d-
51ea-4533-3cd1379a79dc" service="HTTPS" proto=6 action="accept" policyid=1
policytype="proxy-policy" poluuid="1b4276e8-942f-51ec-b92e-ce92797e4550"
policyname="ZTNA-Administrators" duration=10 user="Administrator" group="LDAP-
Administrators" authserver="LDAP-fortiad" gatewayid=1 vip="ZTNA Webserver"
accessproxy="ZTNA Webserver" clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA"
clientdevicetags="on-line/EMS1_ZTNA_FortiAD.info/MAC_EMS1_ZTNA_all_registered_
clients/EMS1_ZTNA_all_registered_clients/MAC_EMS1_ZTNA_FortiAD.info" wanin=127358
rcvdbyte=127358 wanout=3141 lanin=3561 sentbyte=3561 lanout=124521
fctuid="9A016B5A6E914B42AD4168C066EB04CA" appcat="unscanned"
```

8. Verify access to zems.ztnademo.com and zfac.ztnademo.com as well.

Disabling SSL VPN access

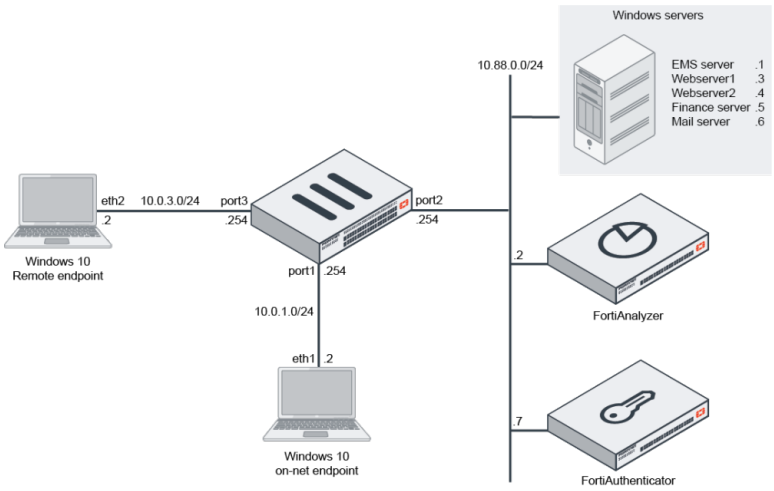
At this point, SSL VPN access can be disabled if you verify your administrators can access the infrastructure devices as configured. However, it is also ok to come back to disabling SSL VPN access after other servers have been migrated. This guide will take the latter approach. See Shut off all SSL VPN access on page 53 for instructions.

Migrate Web access to Finance server for Finance group

Next, migration can be expanded to more users in another control group. This time, the Finance web server 10.88.0.5 which is used by the Finance Team. In the Teleworking setup, this corresponds to the following policy configurations:

```
config firewall policy
    edit 10
        set name "SSL_VPN-Finance"
        set srcintf "ssl.root"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "Webserver" "Finance"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set groups "LDAP-Finance"
    next
end
```

In the above Teleworking configurations, the Webserver address group is also allowed. However, this will be migrated last.



We will use the same access proxy gateway IP and server object as defined in the previous section. In addition, we will need a new FQDN for the Finance server and DNS entry to map to the access proxy.

- Finance server – zfinance.ztnademo.com

DNS configurations

As in the previous section, it is advisable for the FQDN to be defined on an external DNS. In our example, the FortiGate acts as a DNS server for remote clients with A records for mapping the FQDNs to the access proxy address of 10.0.3.10. We will add another entry for zfinance.ztnademo.com in our *Network* > *DNS Servers* > *DNS Database* settings.

DNS Entries

+Create New | Edit | Delete

Type	Details	Status
Address (A)	ems -> 10.0.3.254	Enable
Address (A)	fgt -> 10.0.3.254	Enable
Address (A)	fac -> 10.0.3.7	Enable
Address (A)	mail -> 10.0.3.6	Enable
Address (A)	faz -> 10.0.3.32	Enable
Address (A)	zfaz -> 10.0.3.10	Enable
Address (A)	zems -> 10.0.3.10	Enable
Address (A)	zfac -> 10.0.3.10	Enable
Address (A)	zfinance -> 10.0.3.10	Enable

100% 10

ZTNA server configurations

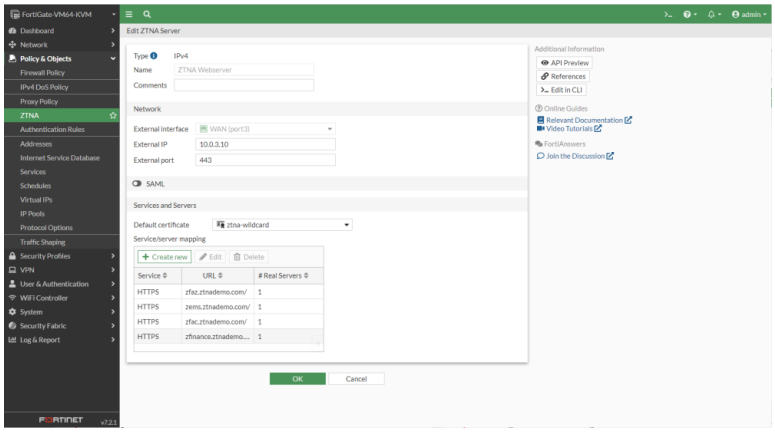
Using the same ZTNA server object from the previous section, define a new HTTPS server mapping for the Finance server.

To add the server mapping from GUI:

1. Under *Policy & Objects* > *ZTNA*, go to the *ZTNA Servers* tab. Edit the *ZTNA Webserver* object.
2. Under *Services/servers mapping*, click *Create new*.
3. For Finance server web access, input the following and click *OK*:

Service	HTTPS
Virtual Host	Specify
Match By	Substring
Host	zfinance.ztnademo.com
Use certificate	1. ztna-wildcard
Servers	Click *Create New*, input the following, and click *OK*: • Type: *IP* • IP: *10.88.0.5* • Port: *9443* • Status: *Active*

4. Click *OK* to finish.



Authentication scheme and rules

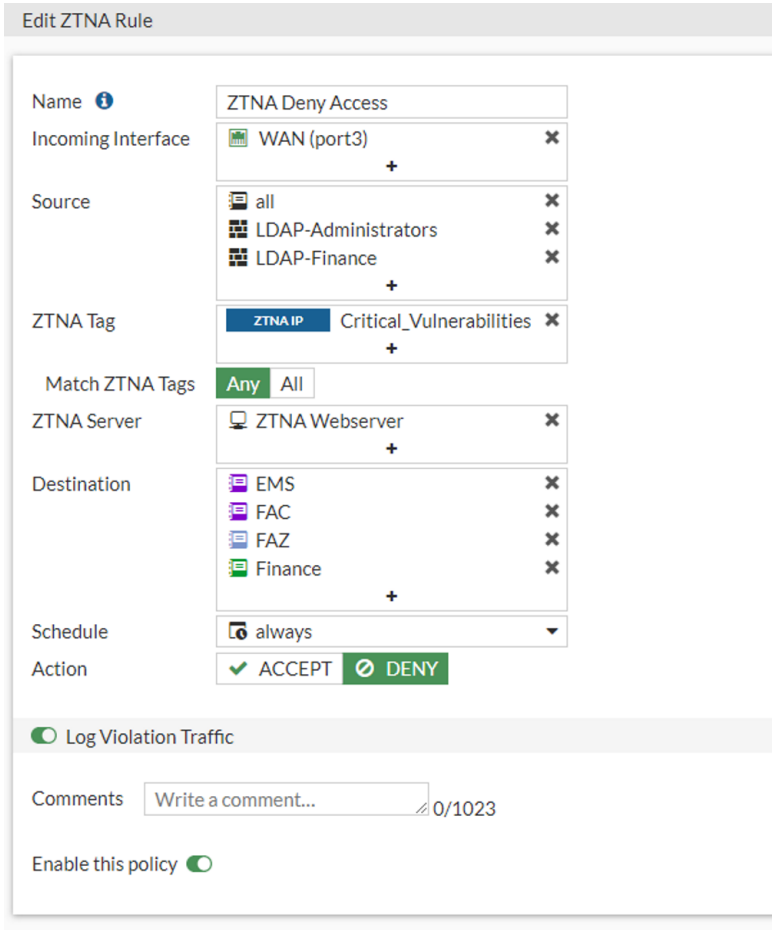
Authentication scheme and rules only need to be configured once if the same authentication applies. The configurations from the previous section suffices for this use case.

ZTNA rule configuration

In this step, we will add the LDAP-Finance user group to the ZTNA Deny Access policy for denying endpoints whose security is compromised. We will also create a rule to allow users who are logged into the FortiAD.Info domain and part of the LDAP-Finance user group to access the Finance server website.

To update the ZTNA Rule for denying access:

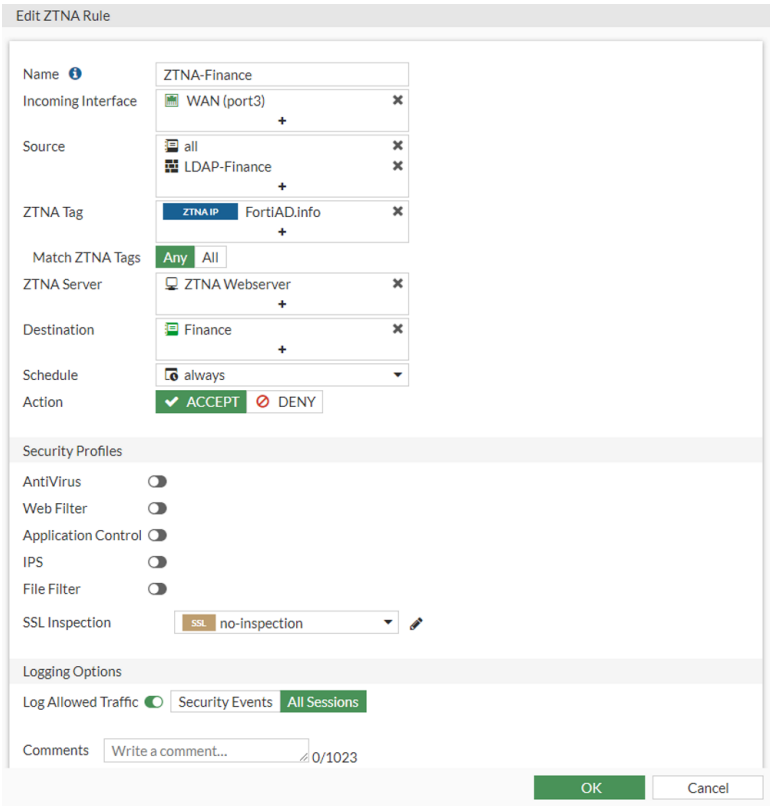
1. In FortiOS, go to *Policy & Objects* > *ZTNA*, click the *ZTNA Rules* tab.
2. Edit the *ZTNA Deny Access* rule.
3. In the *Source* list, add the *User Group LDAP-Finance*.
4. In the *Destination* list, add the *Finance* address object.
5. Click *OK* to complete.



To configure a ZTNA Rule for allowing access:

1. On the *Policy & Objects* > *ZTNA* > *ZTNA Rules* pane, click *Create New*.
2. In the *Name* box, enter `ZTNA-Finance`.
3. In the *Incoming Interface* list, select *WAN (port3)*.
4. In the *Source* list, select the following options:
   - For *Address*, select *all*.
   - For *User*, select *LDAP-Finance*.
5. In the *ZTNA Tag* list, select the *FortiAD.Info* tag.
6. In the *ZTNA Server* list, select *ZTNA Webserver*.
7. In the *Destination* list, select the address objects *Finance*.
8. Beside *Action*, select *Accept*.

9. Enable *Security Profiles* as desired.
10. In the *Logging Options* section, enable *Log Allowed Traffic*, and select *All Sessions*.
11. Enable *Enable this policy*.
12. Click *OK* to complete.



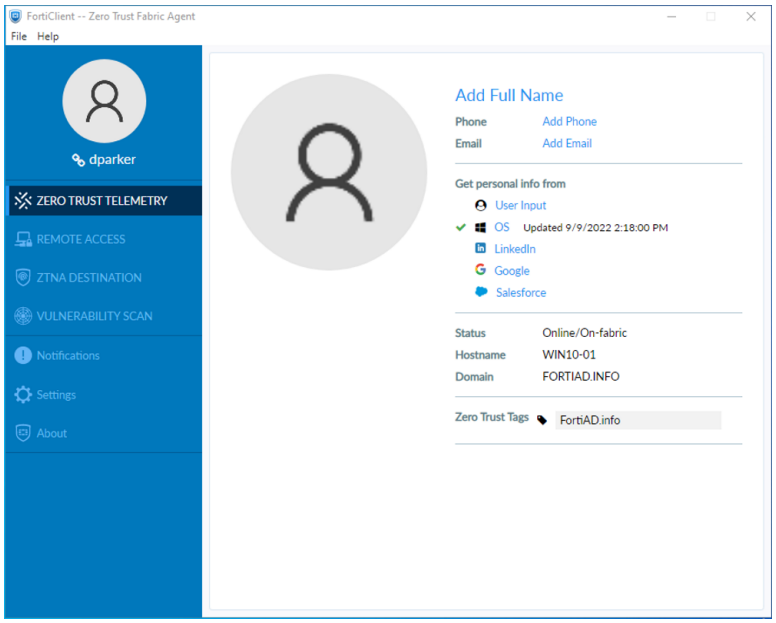
Testing and verification

Once the above configurations are completed, it is time to test ZTNA remote access on a workstation.

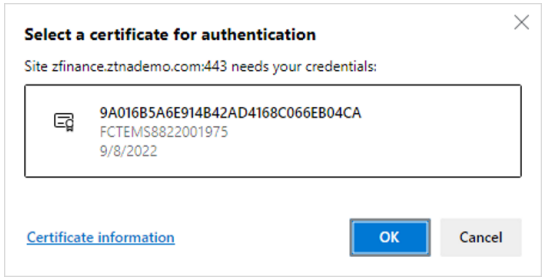
1. Verify access is allowed when user is logged into the FortiAD domain and does not have any Critical vulnerabilities.

To verify access is allowed:

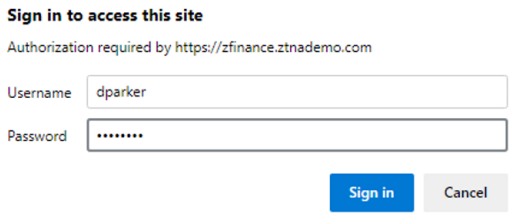
1. On the Finance user dparker's workstation, login to the FortiAD domain.
2. Open the *FortiClient > Zero Trust Telemetry* page.
3. Enter the EMS address or the invitation code. Connect to EMS.
4. Once EMS is connected, click the avatar to identify the current *Zero Trust Tags* assigned to this PC.



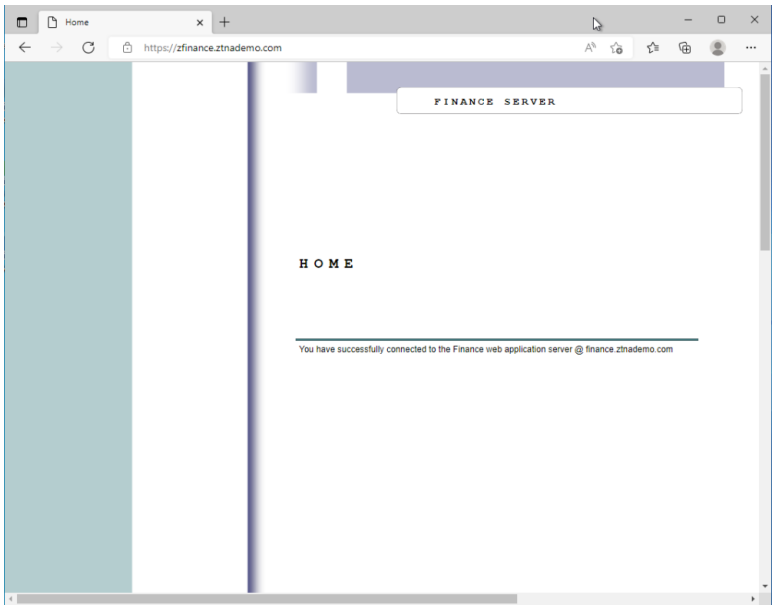
5. Open a browser, and enter the URL https://zfinance.ztnademo.com.
6. The browser will first prompt for the client certificate you want to use for this connection. Select the client certificate and press *OK*.



7. Next, the browser will prompt you for your user credentials. Enter your LDAP/Active Directory to continue.



8. If user authentication passes, the ZTNA rule will then assess the ZTNA tags. Since the user is logged into the FortiAD domain and has no critical vulnerabilities, he can access the Finance website.



9. From the FortiGate, view the corresponding logs under *Log & Report* > *ZTNA Traffic*, or from the CLI:

```
# execute log filter category traffic

# execute log filter field subtype ztna

# execute log display

26 logs found.

10 logs returned.

2.0% of logs has been searched.

1: date=2022-09-09 time=14:39:19 eventtime=1662759559488097013 tz="-0700"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2
srcport=62330 srcintf="port3" srcintfrole="wan" dstcountry="Reserved"
srccountry="Reserved" dstip=10.88.0.5 dstport=9443 dstintf="port2" dstintfrole="dmz"
sessionid=640317 srcuuid="b458a65a-f759-51ea-d7df-ef2e750026d1" service="tcp/9443"
proto=6 action="accept" policyid=3 policytype="proxy-policy" poluuid="509da0ba-3083-
51ed-65ee-fbd7f9e2de24" policyname="ZTNA-Finance" duration=124 user="dparker"
group="LDAP-Finance" authserver="LDAP-fortiad" gatewayid=4 vip="ZTNA Webserver"
accessproxy="ZTNA Webserver" clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA"
clientdevicetags="on-line/MAC_EMS1_ZTNA_all_registered_clients/EMS1_ZTNA_all_registered_
clients/MAC_EMS1_ZTNA_FortiAD.info/EMS1_ZTNA_FortiAD.info" wanin=2305 rcvdbyte=2305
wanout=1136 lanin=1378 sentbyte=1378 lanout=1031
fctuid="9A016B5A6E914B42AD4168C066EB04CA" appcat="unscanned"
```

Disabling SSL VPN access

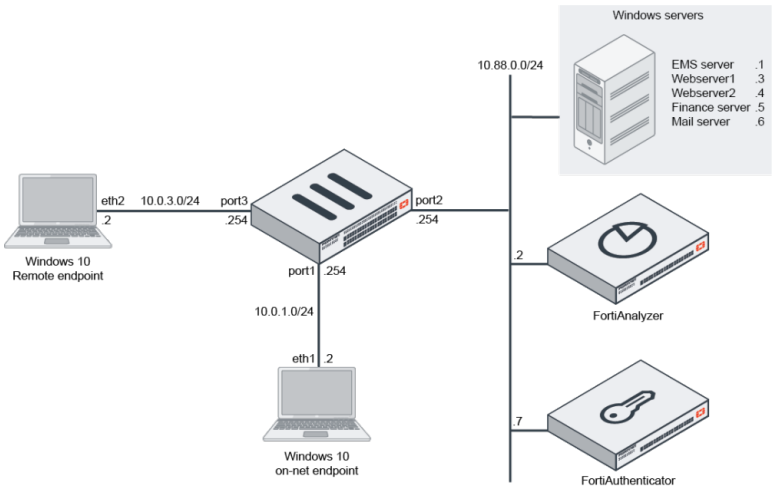
At this point, SSL VPN access can be disabled if you verify other Finance department users can also access the Finance website. However, it is also ok to come back to disabling SSL VPN access after other servers have been migrated. This guide will take the latter approach. See Shut off all SSL VPN access on page 53 for instructions.

Migrate Web access to Webserver1 and Webserver2

Finally, migration can be attempted for the general user base and the resources accessed by all. In the Teleworking setup, this corresponds to the following policy configurations:

```
config firewall policy
    edit 9
        set name "SSL_VPN-Administrators"
        set srcintf "ssl.root"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "EMS" "FAZ" "Webserver" "FAC"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set groups "LDAP-Administrators"
    next
    edit 10
        set name "SSL_VPN-Finance"
        set srcintf "ssl.root"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "Webserver" "Finance"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set groups "LDAP-Finance"
    next
    edit 11
        set name "SSL_VPN-Sales"
        set srcintf "ssl.root"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "Webserver"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
        set groups "LDAP-Sales"
    next
end
```

Since access is allowed for all 3 groups of users, our ZTNA rule will apply to all three LDAP user groups above.



We will use the same access proxy gateway IP and server object as defined in the previous sections. The server object will be mapped to both Webserver1 and Webserver2 using the Round Robin load-balancing algorithm. In addition, we will need a new FQDN for the Webservers and DNS entry to map to the access proxy.

- Web server – zwebserver.ztnademo.com

DNS configurations

As in the previous section, it is advisable for the FQDN to be defined on an external DNS. In our example, the FortiGate acts as a DNS server for remote clients with A records for mapping the FQDNs to the access proxy address of 10.0.3.10. We will add another entry for zwebserver.ztnademo.com in our *Network* > *DNS Servers* > *DNS Database* settings.

DNS Entries

+Create New | Edit | Delete

Type	Details	Status
Address (A)	fgt -> 10.0.3.254	Enable
Address (A)	fac -> 10.0.3.7	Enable
Address (A)	mail -> 10.0.3.6	Enable
Address (A)	faz -> 10.0.3.32	Enable
Address (A)	zfaz -> 10.0.3.10	Enable
Address (A)	zems -> 10.0.3.10	Enable
Address (A)	zfac -> 10.0.3.10	Enable
Address (A)	zfinance -> 10.0.3.10	Enable
Address (A)	zwebserver -> 10.0.3.10	Enable

100% 11

ZTNA server configurations

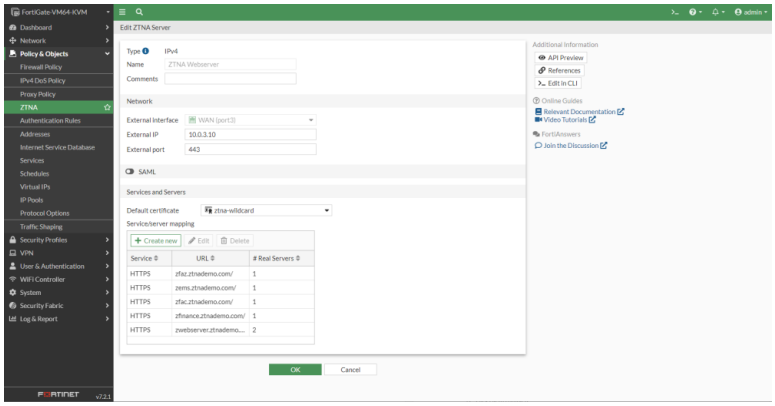
Using the same ZTNA server object from the previous sections, define a new HTTPS server mapping for the Web servers.

To add the server mapping from GUI:

1. Under *Policy & Objects* > *ZTNA*, go to the *ZTNA Servers* tab. Edit the *ZTNA Webserver* object.
2. Under *Services/servers mapping*, click *Create new*.
3. For Finance server web access, input the following and click *OK*:

Service	HTTPS
Virtual Host	Specify
Match By	Substring
Host	zwebserver.ztnademo.com
Use certificate	1. ztna-wildcard
Servers	1. Enable Load balancing and select Round Robin. 2. Click *Create New* to create a mapping to Webserver1, input the following, and click *OK*: • Type: *IP* • IP: *10.88.0.3* • Port: *9443* • Status: *Active* 3. Click *Create New* to create a mapping to Webserver2, input the following, and click *OK*: • Type: *IP* • IP: *10.88.0.4* • Port: *9443* • Status: *Active*

4. Click *OK* to finish.



Authentication scheme and rules

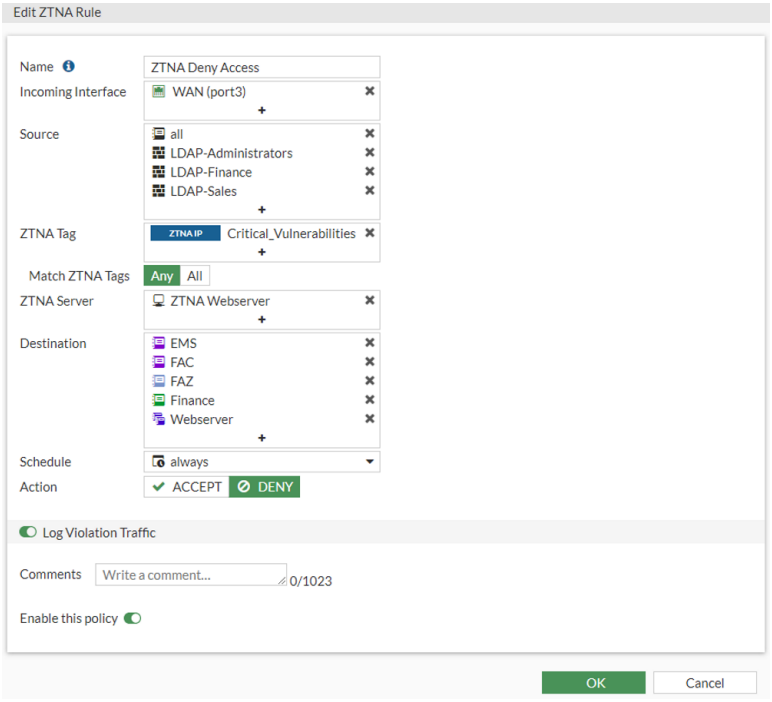
Authentication scheme and rules only need to be configured once if the same authentication applies. The configurations from the previous section suffices for this use case.

ZTNA rule configuration

In this step, we will add the LDAP-Sales user group to the ZTNA Deny Access policy for denying endpoints whose security is compromised. We will also create a rule to allow users who are logged into the FortiAD.Info domain and part of the either the *LDAP-Sales*, *LDAP-Finance* or *LDAP-Administrators* user groups to access the Web server page.

To update the ZTNA Rule for denying access:

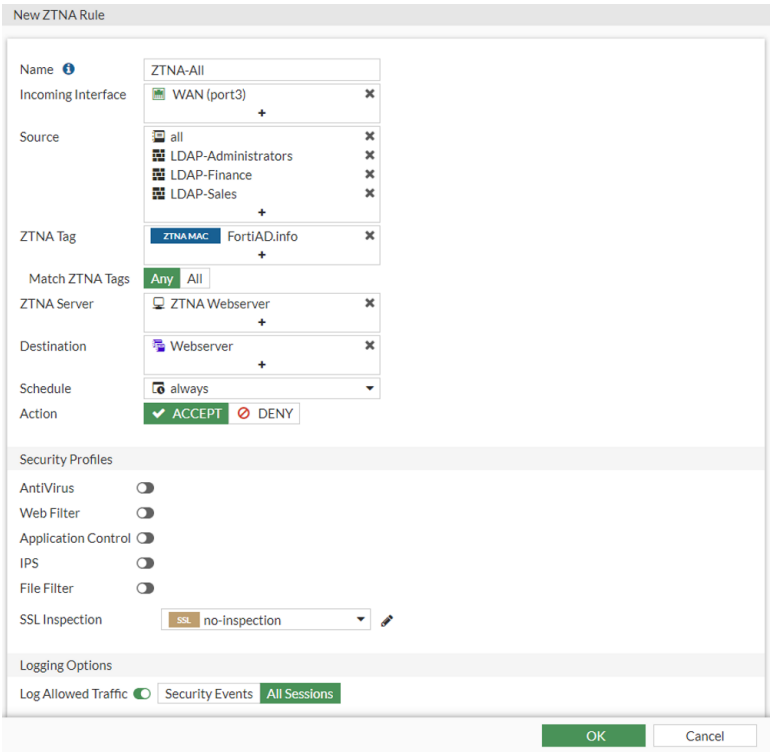
1. In FortiOS, go to *Policy & Objects* > *ZTNA*, click the *ZTNA Rules* tab.
2. Edit the *ZTNA Deny Access* rule.
3. In the *Source* list, add the User Group *LDAP-Sales*.
4. In the *Destination* list, add the *Webserver* address object.
5. Click *OK* to complete.



To configure a ZTNA Rule for allowing access:

1. On the *Policy & Objects* > *ZTNA* > *ZTNA Rules* pane, click *Create New*.
2. In the *Name* box, type *ZTNA-All*.
3. In the *Incoming Interface* list, select *WAN (port3)*.
4. In the *Source* list, select the following options:
   - For *Address*, select *all*.
   - For *User*, select *LDAP-Administrators*, *LDAP-Finance* and *LDAP-Sales*.
5. In the *ZTNA Tag* list, select the *FortiAD.Info* tag.
6. In the *ZTNA Server* list, select *ZTNA Webserver*.
7. In the *Destination* list, select the address objects *Webserver*.
8. Beside *Action*, select *Accept*.

9. Enable *Security Profiles* as desired.
10. In the *Logging Options* section, enable *Log Allowed Traffic*, and select *All Sessions*.
11. Enable *Enable this policy*.
12. Click *OK* to complete.



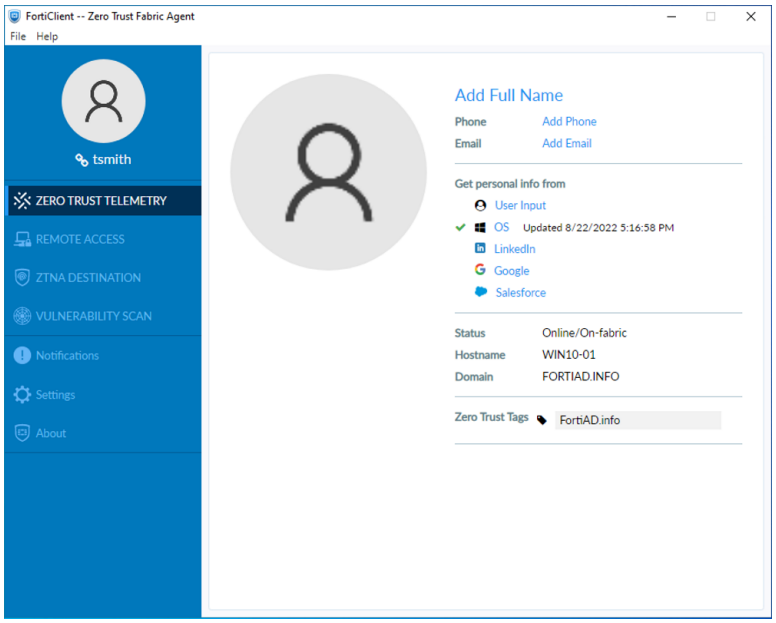
Testing and verification

Once the above configurations are completed, it is time to test ZTNA remote access on a workstation.

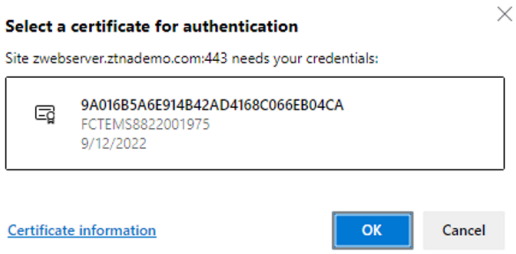
Verify access is allowed when user is logged into the FortiAD domain and does not have any Critical vulnerabilities.

To verify access is allowed:

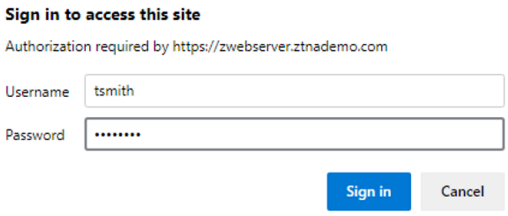
1. On any of workstations belonging to the Administrator, Finance or Sales group, login to the FortiAD domain. In our example, we will use the Sales user Tom Smith (tsmith) as an example.
2. Open the *FortiClient > Zero Trust Telemetry* page.
3. Enter the EMS address or the invitation code. Connect to EMS.
4. Once EMS is connected, click the avatar to identify the current *Zero Trust Tags* assigned to this PC.



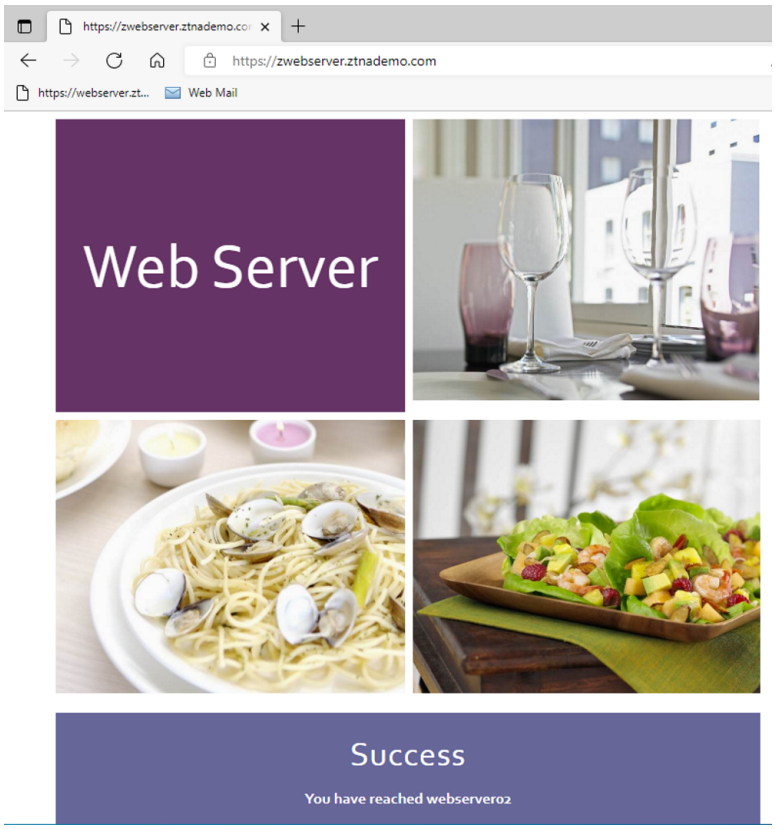
5. Open a browser, and enter the URL https://zwebserver.ztnademo.com.
6. The browser will first prompt for the client certificate you want to use for this connection. Select the client certificate and press *OK*.



7. Next, the browser will prompt you for your user credentials. Enter your LDAP/Active Directory to continue.



8. If user authentication passes, the ZTNA rule will then assess the ZTNA tags. Since the user is logged into the FortiAD domain and has no critical vulnerabilities, he can access the Web server page.



9. Since the page web server is load-balanced, upon refresh and loading another session, the session will load-balance to the other server.
10. From the FortiGate, view the corresponding logs under *Log & Report* > *ZTNA Traffic*, or from the CLI:

```
# execute log filter category traffic

# execute log filter field subtype ztna

# execute log display

21 logs found.

10 logs returned.

2.0% of logs has been searched.

1: date=2022-09-13 time=14:41:55 eventtime=1663105315279744697 tz="-0700"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2
srcport=59715 srcintf="port3" srcintfrole="wan" dstcountry="Reserved"
srccountry="Reserved" dstip=10.88.0.3 dstport=9443 dstintf="port2" dstintfrole="dmz"
sessionid=752775 srcuuid="32b4d66c-9426-51ec-be9c-9b0879d5b527" dstuuid="592dfb72-0775-
51ec-aa79-94bd9894388c" service="tcp/9443" proto=6 action="accept" policyid=4
policytype="proxy-policy" poluuid="8d7e36ec-33a4-51ed-900a-b4c66efa481a"
policyname="ZTNA-All" duration=8 user="tsmith" group="LDAP-Sales" authserver="LDAP-
fortiad" gatewayid=5 vip="ZTNA Webserver" accessproxy="ZTNA Webserver"
clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA" clientdevicetags="on-line/MAC_EMS1_
ZTNA_all_registered_clients/EMS1_ZTNA_all_registered_clients/MAC_EMS1_ZTNA_
FortiAD.info/EMS1_ZTNA_FortiAD.info" wanin=303042 rcvdbyte=303042 wanout=3796 lanin=4993
sentbyte=4993 lanout=304431 fctuid="9A016B5A6E914B42AD4168C066EB04CA" appcat="unscanned"
```

```
2: date=2022-09-13 time=14:40:45 eventtime=1663105245459580873 tz="-0700"
logid="0005000024" type="traffic" subtype="ztna" level="notice" vd="root" srcip=10.0.3.2
srcport=59702 srcintf="port3" srcintfrole="wan" dstcountry="Reserved"
srccountry="Reserved" dstip=10.88.0.4 dstport=9443 dstintf="port2" dstintfrole="dmz"
sessionid=752659 srcuuid="32b4d66c-9426-51ec-be9c-9b0879d5b527" dstuuid="592dfb72-0775-
51ec-aa79-94bd9894388c" service="tcp/9443" proto=6 action="accept" policyid=4
policytype="proxy-policy" poluuid="8d7e36ec-33a4-51ed-900a-b4c66efa481a"
policyname="ZTNA-All" duration=22 user="tsmith" group="LDAP-Sales" authserver="LDAP-
fortiad" gatewayid=5 vip="ZTNA Webserver" accessproxy="ZTNA Webserver"
clientdeviceid="9A016B5A6E914B42AD4168C066EB04CA" clientdevicetags="on-line/MAC_EMS1_
ZTNA_all_registered_clients/EMS1_ZTNA_all_registered_clients/MAC_EMS1_ZTNA_
FortiAD.info/EMS1_ZTNA_FortiAD.info" wanin=303010 rcvdbyte=303010 wanout=3822 lanin=5932
sentbyte=5932 lanout=309087 fctuid="9A016B5A6E914B42AD4168C066EB04CA" appcat="unscanned"
```

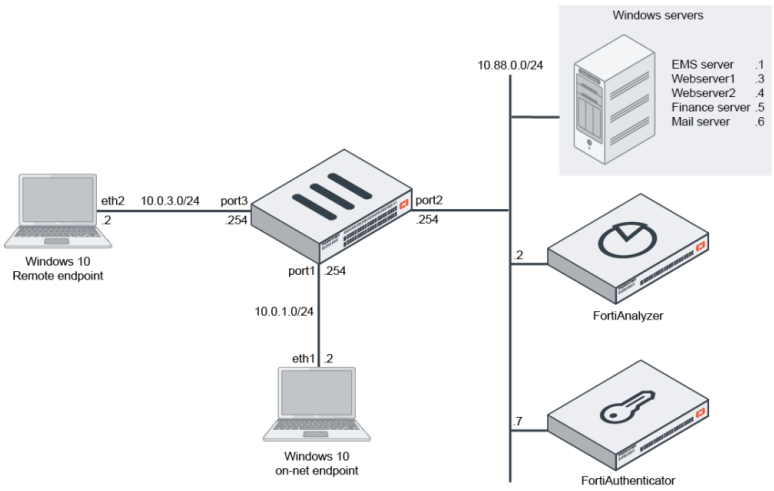
Configuring and verifying rules for on-net access

So far, the configurations are focused on remote off-net access. It is assumed that with prior teleworking setup, on-net access is configured with a wide-open policy as a very basic case. In most scenarios, there will be more segmentation but one variable will remain the same. Access is granted based on the source network and sometimes user login, but the security posture of the device is not checked.

Existing Teleworking configurations to allow traffic from port1 (Clients_LAN) to port2 (DMZ):

```
config firewall policy
    edit 12
        set name "to_DMZ_webservers"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "FAZ" "Finance" "Webserver" "EMS" "FAC"
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set logtraffic all
    next
end
```

In the following section, we will explore configuring on-net access policy with ZTNA tags to enhance the security of on-net devices.



It is assumed that On-net endpoints behind port1 is registered to the FortiClient EMS server over port 8013. Therefore, this port should be allowed without any restrictions.

DNS Configuration

When the users and devices are on-net, the most optimal path to the servers is from port1 (Clients_LAN) to port2 (DMZ). This is the desired path rather than forcing users to access the server through the ZTNA access proxy.

As such, when users access the internal servers using their FQDN addresses, they must resolve to the real IP addresses of the server instead of the access proxy. There are two options to accomplish this.

1. On-net and remote users use the same DNS server. However, the DNS server uses different FQDNs to map to the servers for remote users and on-net users.
2. On-net and remote users use different DNS servers. The same FQDN can be used on the external DNS and internal DNS. However, each DNS will map the server address to a different IP.

In our example, we will use the second approach. For remote users, their DNS server is the FortiGate DNS server, whereas for on-net users, their DNS server is the Windows DNS server.

Explicitly deny access for devices with Critical Vulnerabilities

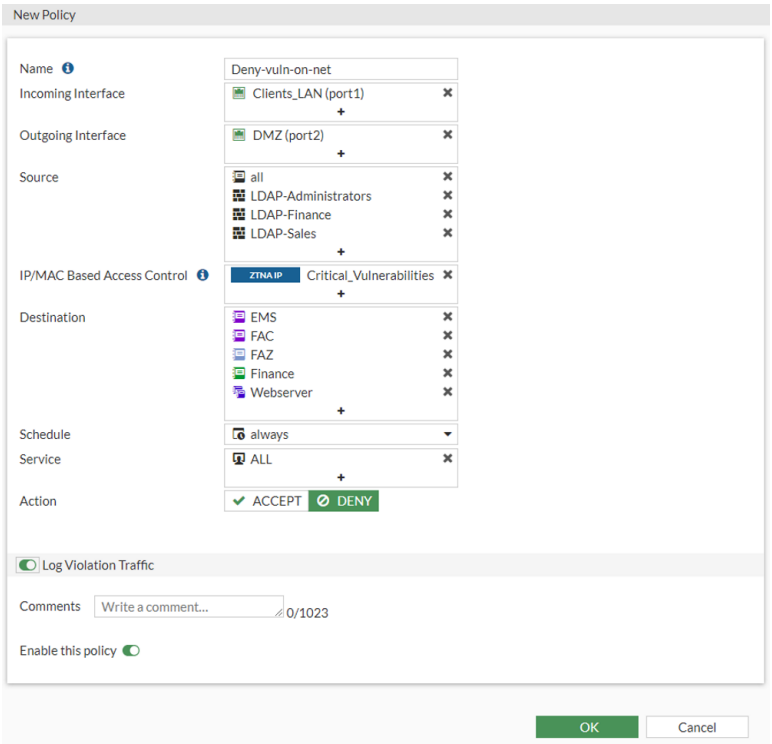
Just like ZTNA access, a Deny rule should be set up to explicitly deny traffic when a device is detected and tagged with Critical Vulnerabilities. In our example, we enable user authentication in order to identify the specific users that are detected, and we'll limit this rule to destination servers defined in ZTNA.

To create a Deny rule for On-net users from port1 (Clients_LAN) to port2 (DMZ):

1. In FortiOS, go to *Policy & Objects* > *Firewall Policy*. Click *Create New*.
2. Name the rule `Deny-vuln-on-net`.
3. In the *Incoming interface*, select *port1*.
4. In the *Outgoing interface*, select *port2*.
5. In the *Source* list:

- Select the Address *all*.
- Add the User Groups *LDAP-Administrators*, *LDAP-Finance* and *LDAP-Sales*.

6. In the *IP/MAC Based Access Control* field, add the *Critical_Vulnerabilities* tag.
7. In the *Destination* list, add the *EMS*, *FAC*, *FAZ*, *Finance* and *Webserver* address objects.
8. Set the *Service* to *ALL*.
9. Set the *Action* to *DENY*.
10. Enable *Log Violation Traffic*.
11. Click *OK* to complete.



12. Place this rule in front of the existing *to_DMZ_webservers* firewall policy.

Allow access to servers based on group

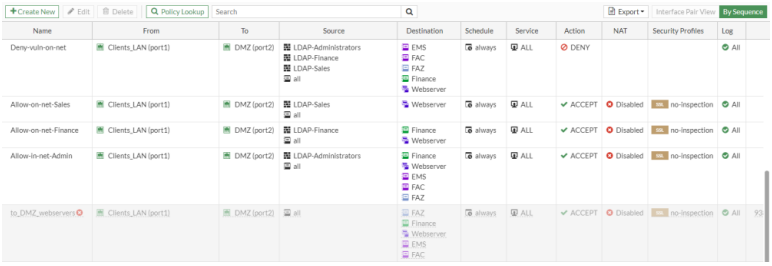
Next, create new rules to allow each user group access to their servers.

To create Allow rules for On-net users from port1 (Clients_LAN) to port2 (DMZ):

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Click *Create New*. Name the first rule `Allow-on-net-Sales`.
   a. In the *Incoming interface*, select *port1*.
   b. In the *Outgoing interface*, select *port2*.
   c. In the *Source* list:
      - Select the Address *all*.
      - Add the User Groups *LDAP-Sales*.
   d. In the *IP/MAC Based Access Control* field, add the *FortiAD.info* tag.

e. In the *Destination* list, add the *Webserver* address object.
f. Set the *Service* to *ALL*.
g. Set the *Action* to *ACCEPT*.
h. Set *Inspection Mode* to *Proxy-based*.
i. Enable *NAT* where necessary.
j. Enable *Security Profiles* as needed.
k. Enable *Log Allowed Traffic*, and choose *All Sessions*.
l. Click *OK* to complete.

3. Click *Create New*. Name the 2nd rule `Allow-on-net-Finance`.
   a. In the *Incoming interface*, select *port1*.
   b. In the *Outgoing interface*, select *port2*.
   c. In the *Source* list:
      - Select the Address *all*.
      - Add the User Groups *LDAP-Finance*.
   d. In the *IP/MAC Based Access Control* field, add the *FortiAD.info* tag.
   e. In the *Destination* list, add the *Finance* and *Webserver* address objects.
   f. Set the *Service* to *ALL*.
   g. Set the *Action* to *ACCEPT*.
   h. Set *Inspection Mode* to *Proxy-based*.
   i. Enable *NAT* where necessary.
   j. Enable *Security Profiles* as needed.
   k. Enable *Log Allowed Traffic*, and choose *All Sessions*.
   l. Click *OK* to complete.
4. Click *Create New*. Name the 3rd rule `Allow-on-net-Admin`.
   a. In the *Incoming interface*, select *port1*.
   b. In the *Outgoing interface*, select *port2*.
   c. In the *Source* list:
      - Select the Address *all*.
      - Add the User Groups *LDAP-Administrators*.
   d. In the *IP/MAC Based Access Control* field, add the *FortiAD.info* tag.
   e. In the *Destination* list, add the *EMS*, *FAC*, *FAZ*, *Finance* and *Webserver* address objects.
   f. Set the *Service* to *ALL*.
   g. Set the *Action* to *ACCEPT*.
   h. Set *Inspection Mode* to *Proxy-based*.
   i. Enable *NAT* where necessary.
   j. Enable *Security Profiles* as needed.
   k. Enable *Log Allowed Traffic*, and choose *All Sessions*.
   l. Click *OK* to complete.
5. Place the new policies below the *Deny-vuln-on-net* policy but above the *to_DMZ_webservers* policy.
6. Disable the *to_DMZ_webservers* policy so that authentication does not fall through to this wide open policy.



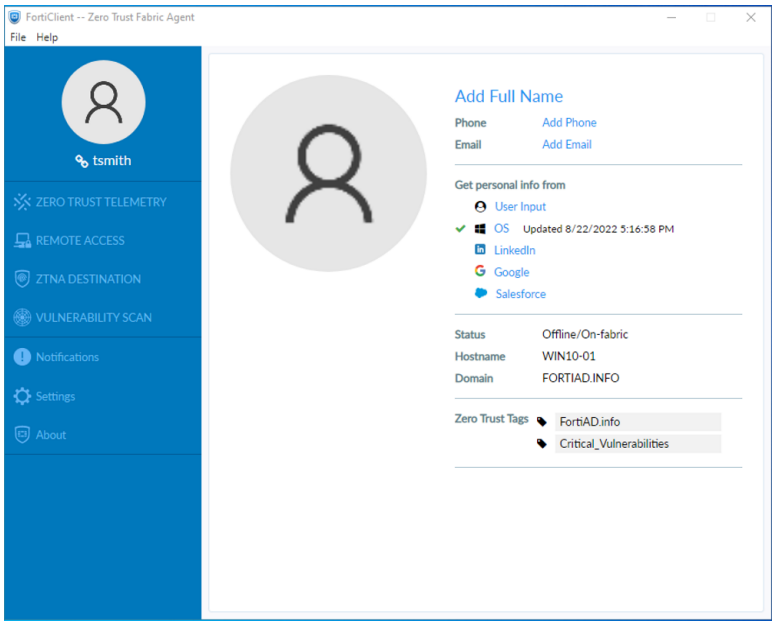
Testing and verification

Once the above configurations are completed, it is time to test On-net access on a workstation. Two test cases will be performed.

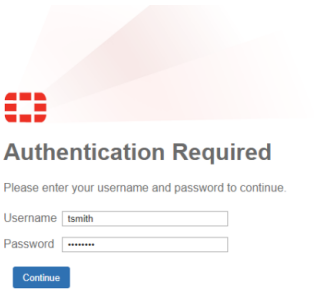
1. Verify access is denied when Critical Vulnerabilities are present on the PC
2. Verify access is allowed when Critical Vulnerabilities are resolved, and user is logged into the FortiAD domain.

To verify access is denied:

1. On a workstation that is on-net, login to the FortiAD domain. In our example, we will use user Tom Smith (tsmith) from the Sales group logging into his PC 10.0.1.2.
2. Open the *FortiClient > Zero Trust Telemetry* page.
3. Enter the EMS address or the invitation code. Connect to EMS.
4. Once EMS is connected, click the avatar to identify the current *Zero Trust Tags* assigned to this PC. This PC currently has *Critical Vulnerabilities* detected.



5. Open a browser, and enter the URL https://zwebserver.ztnademo.com.
6. The browser will redirect you to firewall policy authentication. Authenticate with the tsmith user. Note that firewall authentication can be triggered with HTTP/80, HTTPS/443 and SSH/22 access. If using ports other than these, you may need to trigger authentication with the above ports first.



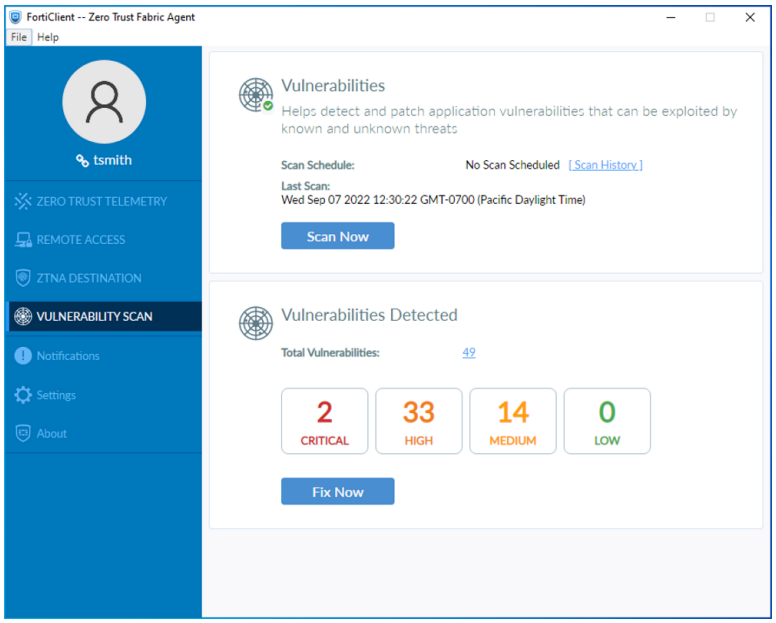
7. If user authentication passes, the ZTNA tags will be assessed. Since this workstation has Critical Vulnerabilities, access to the Web server is denied. There are no replacement messages for firewall policy authentication failures.
8. On the FortiGate, view the corresponding logs under Log & Report > Forward Traffic, or from the CLI:

```
# execute log filter category traffic

# execute log filter field subtype policy

# execute log display

3802 logs found.

10 logs returned.

2.0% of logs has been searched.

15: date=2022-09-13 time=16:53:42 eventtime=1663113222809282854 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.0.1.2 srcport=51842 srcintf="port1" srcintfrole="undefined" dstip=10.88.0.3
dstport=443 dstintf="port2" dstintfrole="dmz" srcuuid="b458a65a-f759-51ea-d7df-
ef2e750026d1" dstuuid="592dfb72-0775-51ec-aa79-94bd9894388c" srccountry="Reserved"
dstcountry="Reserved" sessionid=764033 proto=6 action="deny" policyid=13
policytype="policy" poluuid="d62c92aa-33b1-51ed-a603-bc6e64fb9e67" policyname="Deny-
vuln-on-net" user="tsmith" authserver="LDAP-fortiad" service="HTTPS" trandisp="noop"
duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned" crscore=30
craction=131072 crlevel="high"craction=131072 crlevel="high"
```

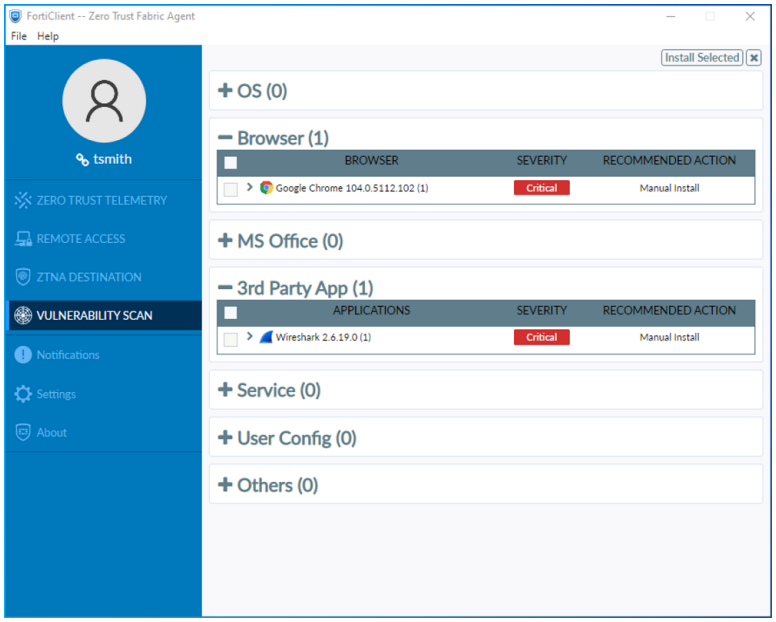
9. For other users and device with Critical vulnerabilities, try accessing internal server resources as well.

To verify access is allowed:

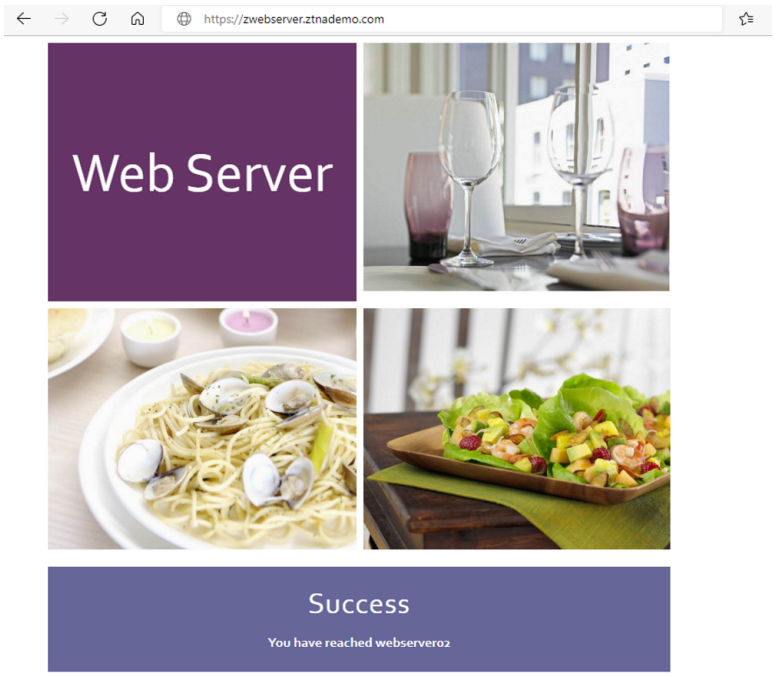
1. Open the *FortiClient* > *Vulnerability Scan* page.



2. Click on *Critical* to see the Application that has been identified with a critical vulnerability.



3. Apply the necessary fix to remove the vulnerability. Then perform a vulnerability scan.
4. Now that the workstation does not have a critical vulnerability, open your browser again to try accessing the web server again.
5. Open a browser, and enter the URL https://zwebserver.ztnademo.com.
6. If prior user authentication is still valid, you will have access to the web server right away. In not, enter your user credentials. You should be able to access your web server.



7. From the FortiGate, view the corresponding logs under *Log & Report* > *ZTNA Traffic*, or from the CLI:

```
# execute log filter category traffic

# execute log filter field subtype policy

# execute log display

3913 logs found.

10 logs returned.

2.0% of logs has been searched.

11: date=2022-09-13 time=17:06:54 eventtime=1663114014269608499 tz="-0700"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
srcip=10.0.1.2 srcport=51878 srcintf="port1" srcintfrole="undefined" dstip=10.88.0.3
dstport=443 dstintf="port2" dstintfrole="dmz" srcuuid="b458a65a-f759-51ea-d7df-
ef2e750026d1" dstuuid="592dfb72-0775-51ec-aa79-94bd9894388c" srccountry="Reserved"
dstcountry="Reserved" sessionid=764718 proto=6 action="close" policyid=14
policytype="policy" poluuid="4f530284-33b4-51ed-d838-73d540cb3b21" policyname="Allow-on-
net-Sales" user="tsmith" group="LDAP-Sales" authserver="LDAP-fortiad" service="HTTPS"
trandisp="noop" duration=1 sentbyte=1523 rcvdbyte=1410 sentpkt=7 rcvdpkt=8
appcat="unscanned
```

8. Verify access for other On-net users as well.

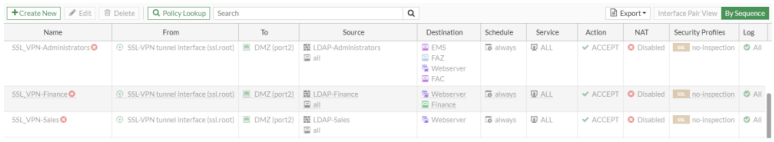
Shut off all SSL VPN access

So far, SSL VPN access is still allowed in case users have not fully migrated. Upon a successful verification that users have access to the web resources through ZTNA, SSL VPN configurations can be disabled.

Without completely wiping out SSL VPN settings, admins can first disable current SSL VPN policies that give access to remote users.

To disable SSL VPN policies:

1. On the FortiGate, go to *Policies & Objects* > *Firewall Policy*.
2. Locate the SSL VPN policies. In our example, these are:
   - *SSL_VPN-Administrators*
   - *SSL_VPN-Finance*
   - *SSL_VPN-Sales*
3. Right click on each of these policies and set *Status* to *disable*.



4. Remote users will no longer have access to SSL VPN.

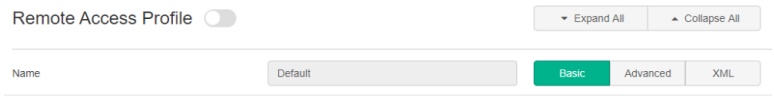
In case that you will not require any SSL VPN connections for any other remote users, and you would like to disable SSL VPN and listening on the SSL VPN port.

To disable all SSL VPN connections:

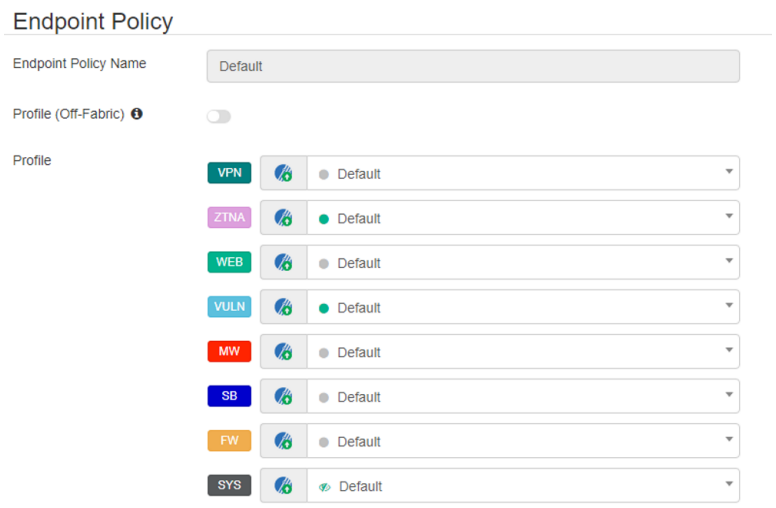
1. On the FortiGate, go to *VPN* > *SSL-VPN Settings*.
2. Toggle *Enable SSL-VPN* from *Enable* to *Disable.*
3. Click *Apply* to save the settings.

To disable the Remote Access module on FortiClient:

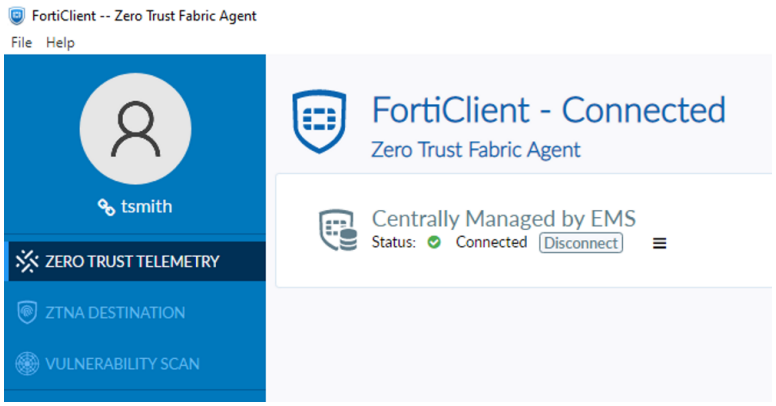
1. On the FortiClient EMS, go to *Endpoint Profiles* > *Remote Access*.
2. Click on the *Default* profile and click *Edit*.
3. At the top, toggle the *Remote Access Profile* from *enable* to *disable*.



4. Click *Save* to complete.
5. Go to *Endpoint Policy & Components* > *Manage Policies*.
6. Click on the *Default policy* and click *Edit*.
7. Verify that VPN is now disabled in the *Profile* section.



8. On a workstation connected to the EMS, the changes will be pushed to it shortly. Verify that the *Remote Access* module is no longer present.



Conclusion

This concludes the SSL VPN teleworking to ZTNA migration for Hosted Web resources.

To recap:

- FortiClient EMS was updated to add the ZTNA module and enable new ZTNA tagging rules
- FortiGate was connected to the FortiClient EMS via the Fabric Connector
- Hosted web resources were migrated one by one based on the user groups that are allowed to access them
  - Web resources belonging to the Administrator group was migrated first, since it only affected Administrators
  - Web resources belonging to the Finance group was migrated next, since it only affected the Finance team
  - Web resources that were accessible to all were migrated last
- During each migration step, access was tested to verify each group was still able to access the migrated web resources remotely

- For On-net use cases, policies were created to verify the security postures of devices in order to prevent vulnerable devices from accessing web resources
- Finally, SSL VPN access was removed once ZTNA access have been verified

These steps represent the process for migrating a basic SSL VPN teleworking setup. They also lay the foundation for building more scalable networks based on role based access control and security postures that you define with EMS's Zero Trust Tagging Rules. For information on more security posture checks, see the Endpoint Posture Check reference guide.

More information

The following product models and firmware were used in this guide:

Product	Model	Firmware
FortiGate	FortiGate-VM	FortiOS 7.2.1
FortiClient	FortiClient Windows	7.0.6
FortiClient EMS	FortiClient EMS	7.0.6

Documentation references

Feature documentation

- FortiOS Admin Guide
  - ZTNA Chapter
- FortiClient EMS Admin Guide
  - Zero Trust Tags
- FortiClient Admin Guide
- Endpoint Posture Check Reference

Solution hub

https://docs.fortinet.com/ztna

4-D resources

https://docs.fortinet.com/4d-resources/ZTNA

Marketing and datasheets

- Next-Generation Firewall
- FortiClient Endpoint Security Overview

www.fortinet.com